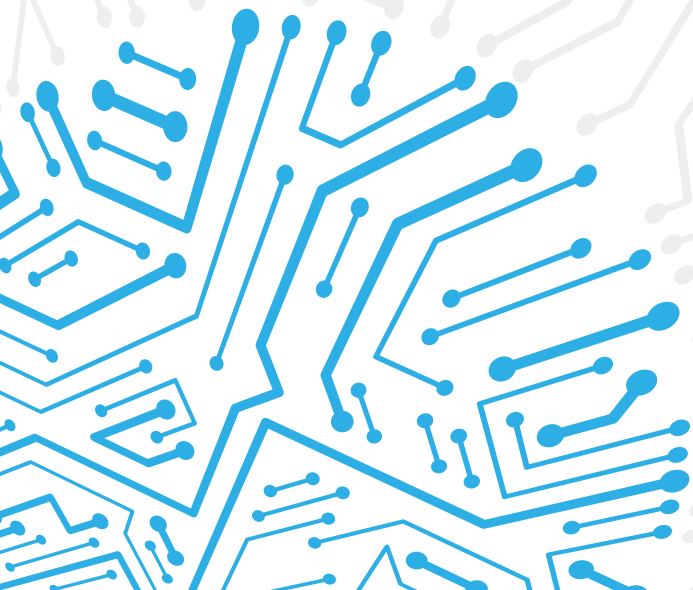
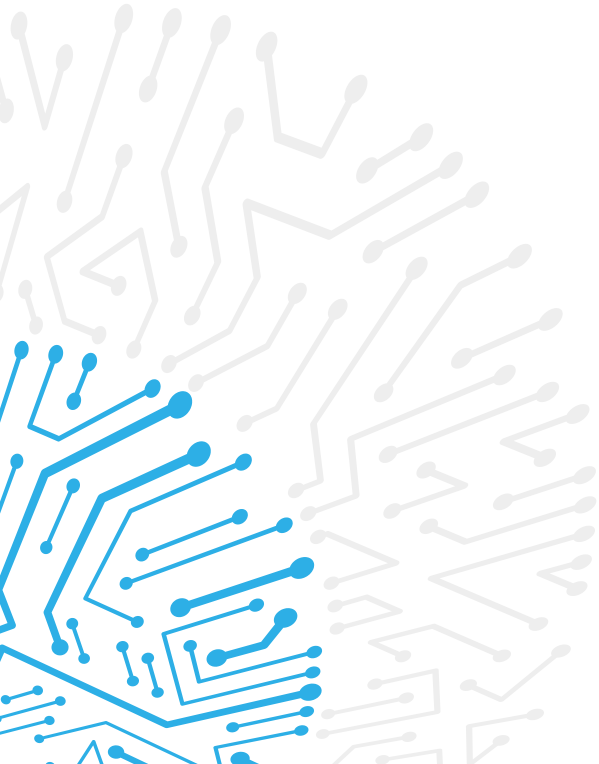
NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

ZPRÁVA O STAVU KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY ZA ROK 2022





ZPRÁVA O STAVU KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY ZA ROK 2022


NÚKIB
Národní úřad
pro kybernetickou
a informační
bezpečnost

Úvodní slovo ředitele

Vážené dámy, vážení pánové,

před Vámi je jubilejní, již desátá Zpráva o stavu kybernetické bezpečnosti České republiky. Obdobně jako v předchozích letech, přinesl také rok 2022 nové výzvy a bohužel i nové hrozby. Jeho hlavní událostí byla jednoznačně ruská invaze na Ukrajinu, jež započala dne 24. února, a která zásadním způsobem změnila bezpečnostní situaci na našem kontinentu. Dopady tamního ozbrojeného konfliktu měly bezpochyby vliv také na dění v kyberprostoru.

Posláním Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) je zajišťovat kybernetickou bezpečnost České republiky. Na plnění tohoto úkolu jsme také v roce 2022 usilovně pracovali. Kontinuálně jsme se věnovali řešení dopadů kybernetických útoků a jejich prevenci. Účastnili jsme se řady domácích a zahraničních akcí, organizovali jsme cvičení, školení, semináře či konference a soustavně pracovali na osvětě a vzdělávání veřejnosti i našich zaměstnanců. To vše s jedním jediným cílem. Udělat z České republiky bezpečnější místo pro život.

Jednou z velkých výzev pro náš stát bylo předsednictví v Radě EU ve druhé polovině minulého roku, na němž se NÚKIB, spolu s celou řadou dalších tuzemských institucí, podílel. NÚKIB se podařilo naplnit všechny tři stanovené priority. Nalezli jsme shodu napříč členskými státy ohledně podoby návrhu nařízení Evropského parlamentu a Rady EU, který stanoví opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti v orgánech, institucích a jiných subjektech EU. Jednali jsme o návrhu Aktu o kybernetické odolnosti (Cyber Resilience Act) a v neposlední řadě se nám povedlo také zviditelnit téma kybernetické bezpečnosti dodavatelského řetězce v informačních a komunikačních technologiích.

Nad rámec velkého množství námi vedených jednání jsme organizovali řadu vzdělávacích a společenských akcí, kterých se fyzicky či virtuálně zúčastnily stovky lidí nejen z EU. Bez jakýchkoliv pochyb mohu prohlásit, že Česká republika i NÚKIB svou roli zvládly skvěle, o čemž svědčí také reakce našich evropských partnerů. Během šesti měsíců pod naším vedením udělala EU v oblasti kybernetické bezpečnosti skutečně velký krok kupředu. Zároveň jsme prokázali, že české instituce zvládají pracovat jako jeden tým. V tomto kriticky důležitém období, během kterého se na naši zemi obrátila pozornost celé Evropy a spojenců, tak Česká republika jednoznačně obstála.

Stejně jako kyberprostor nezná hranic, tak kybernetická bezpečnost nezná konce a není jen o některých z nás. V moderním a stále více digitálním světě se týká nás všech. Abychom byli úspěšní a svět i lidé okolo nás byli v bezpečí, neobejdeme se bez vzájemné spolupráce a komunikace. A právě spolupráce byla v uplynulém roce jako již tradičně jednou z hlavních činností NÚKIB. Ať už se jedná o spolupráci na mezinárodní úrovni s unijními a aliančními partnery, domácí koordinaci s partnery mnoha různých celků, ale i o spolupráci s našimi konstituenty. Velice si proto cením všech kvalitních vztahů a spojenectví, která se nám daří budovat a posilovat.

Na závěr bych rád poděkoval 317 organizacím, které se formou vypracování našich dotazníků podílely na přípravě této Zprávy. Vaší důvěry i zpětné vazby si velmi vážíme. I tímto způsobem dáváte najevo, že Vám není bezpečnost České republiky lhostejná a že jste odhodláni se na ní podílet. Soudržnost a spolupráce jsou klíčovými složkami k zajištění bezpečnosti všech našich spoluobčanů.

Lukáš Kintr

Shrnutí Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2022

- **Během roku 2022 došlo k mírnému snížení kybernetických incidentů evidovaných NÚKIB ze 157 na 146, nicméně Policie České republiky zaznamenala téměř dvojnásobný nárůst kyberkriminálních aktivit.** Největší hrozbu pro kybernetickou bezpečnost České republiky pak i nadále představují aktivity státem sponzorovaných kybernetických aktérů a činnost kyberkriminálních uskupení.

- Mezi nejčastější typy útoků během uplynulého roku patřily různé druhy phishingu, spear-phishingu, vishingu a podvodných e-mailů či útoky na dostupnost, převážně formou DDoS útoků. Naopak méně často se vyskytovalo zneužívání zranitelností či ransomwarové útoky, které však i nadále představují relevantní hrozbu. **NÚKIB zároveň evidoval i několik incidentů v souvislosti s ruskou invazí na Ukrajinu.**

- Nejvíce kybernetických incidentů NÚKIB evidoval v rámci veřejného sektoru, následně zdravotnictví a soukromého sektoru. **NÚKIB také zaznamenal významný, a to téměř dvojnásobný, nárůst incidentů v rámci kritické informační infrastruktury, přičemž většinu z nich tvořily útoky na dostupnost služeb.**

- NÚKIB během roku 2022 vydal celkem 16 upozornění a 3 varování v kontextu aktuálních hrozeb či zranitelností. **Některá varování poté přímo souvisela s riziky plynoucími z ruské invaze na Ukrajinu.**

- **Značná část agendy NÚKIB během roku 2022 spočívala v podílení se na přípravách a realizaci českého předsednictví v Radě Evropské unie** (dále jen „CZ PRES“)**.** Významná byla především spolupráce v kontextu nové směrnice NIS 2, která byla přijata právě během CZ PRES. I mimo toto období však NÚKIB intenzivně spolupracoval s partnery v EU a NATO na zajišťování kybernetické bezpečnosti a rozvíjel mezinárodní spolupráci.

- **Významný proces z pohledu kybernetické bezpečnosti na národní úrovni, který započal v roce 2022, představuje příprava návrhu nového zákona o kybernetické bezpečnosti, jež s výše zmíněnou směrnicí NIS 2 úzce souvisí.** V rámci přípravy na tuto legislativní změnu, jejíž účinnost se předpokládá od podzimu 2024, bylo zřízeno pět interních expertních skupin, ve kterých přes více než 40 zaměstnanců NÚKIB připravilo návrh nového zákona o kybernetické bezpečnosti a jeho prováděcích předpisů.

- V neposlední řadě se NÚKIB intenzivně věnoval i osvětové činnosti a organizaci kybernetických cvičení. Velká část osvětových projektů probíhala v rámci vzdělávacího sektoru. Jejich cílem bylo mimo jiné zvýšení povědomí o současných kybernetických hrozbách a vytváření podmínek pro vzdělávání budoucích expertů v oblasti kybernetické bezpečnosti. **Během roku taktéž proběhlo sedm domácích a tři mezinárodní cvičení kybernetické bezpečnosti, mimo jiné i sektorově zaměřené cvičení Health Czech pro organizace zdravotnického sektoru.**

Obsah

Seznam použitých zkratek

CIRC – Computer Incident Response Capability

CZ PRES – Předsednictví České republiky v Radě Evropské unie

ČR – Česká republika

DoS/DDoS – Denial of Service / Distributed Denial of Service

ENISA – Agentura Evropské unie pro kybernetickou bezpečnost

EU – Evropská unie

ISZS – Informační systém základní služby

ITU – Mezinárodní telekomunikační unie (International Telecommunication Union)

KII – Kritická informační infrastruktura

NATO – Severoatlantická aliance

NIS – Network and Information Security

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

OBSE – Organizace pro bezpečnost a spolupráci v Evropě

OECD – Organizace pro ekonomickou spolupráci a rozvoj
(Organisation for Economic Co-operation and Development)

OSN – Organizace spojených národů

PZS – Provozovatel základní služby

VIS – Významný informační systém

2022: Kybernetická bezpečnost ČR v datech

764
hlášení kybernetických incidentů obdržených NÚKIB

146
kybernetických incidentů řešených NÚKIB

3
velmi významné kybernetické incidenty řešené NÚKIB

2 067
bezpečnostních incidentů řešených CSIRT.CZ – národním bezpečnostním týmem ČR

1 425
řešených phishingových útoků CSIRT.CZ

18 554
trestných činů v oblasti kybernetické kriminality a kriminality páchané na internetu

504
účastníků cvičení kybernetické bezpečnosti uspořádaných NÚKIB

10
cvičení kybernetické bezpečnosti provedených NÚKIB

51 686
proškolených uživatelů kurzy NÚKIB

66
subjektů kritické informační infrastruktury

128
informačních a komunikačních systémů kritické informační infrastruktury

193
správců a provozovatelů významných informačních systémů

588
významných informačních systémů

155
provozovatelů základní služby

192
informačních systémů základní služby

O dokumentu

NÚKIB na začátku roku 2023 rozeslal dotazník se 77 otázkami, a to jak subjektům regulovaným zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, tak i řadě dalších klíčových institucí a organizací, které zákonem o kybernetické bezpečnosti regulovány nejsou. Otázky se týkaly širokého záběru témat, například kybernetických útoků, nákladů na kybernetickou bezpečnost, personálních kapacit v oblasti kybernetické bezpečnosti, uživatelů, technologií i zavedených procesů. Dotazník vyplnilo celkem 317 subjektů, z toho 236 regulovaných a 81 neregulovaných. Ze získaných dat NÚKIB čerpal informace pro potřeby Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2022 (dále také jen „Zpráva“). Veškeré údaje z dotazníků jsou anonymizovány.

Proces hodnocení

Hodnocení stavu kybernetické bezpečnosti v ČR je založeno na analytickém procesu, který zahrnuje kvantitativní i kvalitativní vyhodnocení dat z vyplněných dotazníků, poznatky NÚKIB, informace poskytnuté partnery a další dostupné informace z otevřených zdrojů. NÚKIB neměl možnost data poskytnutá respondenty kontrolovat, ani hlouběji ověřovat uvedená tvrzení. Analytické závěry obsažené ve Zprávě jsou založeny na premise, že odpovědi v dotaznících nejsou zkresleny. K vyjádření analytického hodnocení používáme pravděpodobnostní výrazy (viz níže).

Zpráva neposkytuje vyčerpávající seznam všech aktivit v oblasti kybernetické bezpečnosti. Účelem dokumentu je popsat a vyhodnotit hrozby v kybernetickém prostoru, s nimiž se ČR v roce 2022 potýkala, stejně jako aktivity, které napomáhají jejich zmírnění.

Pravděpodobnostní výrazy použité ve Zprávě o stavu kybernetické bezpečnosti České republiky za rok 2022

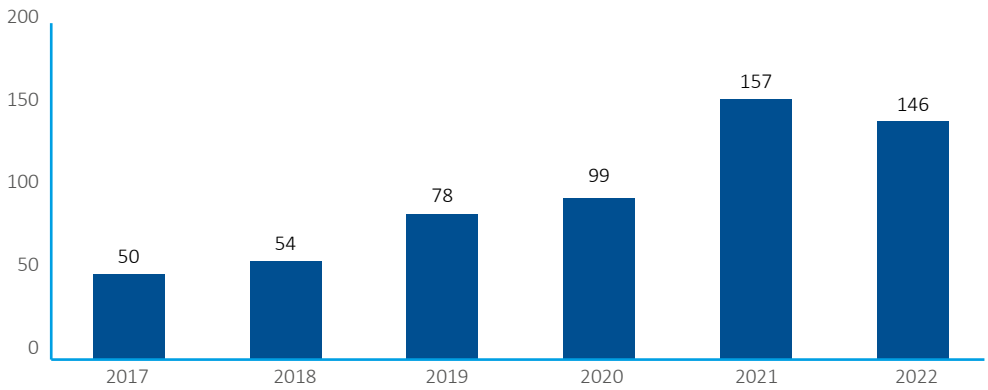
Pravděpodobnostní výrazy a vyjádření jejich procentuálních hodnot:

VÝRAZ	PRAVDĚPODOBNOST
Téměř jistě	90–100 %
Velmi pravděpodobně	75–85 %
Pravděpodobně	55–70 %
Nelze vyloučit / Reálná možnost	25–50 %
Nepravděpodobně	15–20 %
Velmi nepravděpodobně	0–10 %

KYBERNETICKÁ BEZPEČNOST ČR V ROCE 2022 Z POHLEDU NÚKIB[1]

Počet kybernetických bezpečnostních incidentů v roce 2022 registrovaných NÚKIB

V roce 2022 obdržel NÚKIB celkem 764 hlášení od regulovaných i neregulovaných osob podle zákona o kybernetické bezpečnosti, z nichž 146 vyhodnotil jako kybernetické bezpečnostní incidenty, které následně řešil. **Navzdory značnému nárůstu hlášení došlo v roce 2022 k mírnému meziročnímu poklesu evidovaných incidentů**.

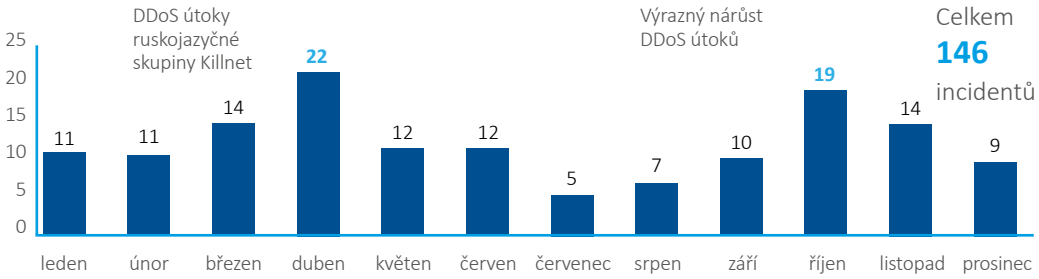


Graf 1: Vývoj počtu incidentů registrovaných NÚKIB

Jedním z pravděpodobných důvodů poklesu incidentů je mj. skutečnost, že v roce 2022 neproběhla žádná významnější kampaň, při níž by docházelo k masivnímu zneužívání konkrétní zranitelnosti. Oproti tomu v roce 2021 proběhly kampaně zneužívající zranitelností ProxyLogon a ProxyShell, jejichž cílem byla široce využívaná služba Microsoft Exchange Server, a ke konci roku 2021 byla objevena zranitelnost Log4Shell. Do jisté míry klesla také proaktivita ze strany NÚKIB (realizace tzv. threat huntingu, kdy jsou incidenty aktivně vyhledávány), což bylo dáno především personálními kapacitami. V obecnější rovině je pak nutné brát v potaz, že NÚKIB ani samotné subjekty nemají možnost detekovat všechny incidenty. Zejména **velmi závažné typy útoků je nesmírně složité detekovat,** neboť útočníci vynakládají mimořádné úsilí, aby zůstali nepozorovaní. Některé organizace taktéž nemusí řádně kybernetický bezpečnostní incident identifikovat, případně se mohou rozhodnout detekovaný incident NÚKIB nenahlásit. **V kontextu rostoucí míry kyberkriminality či incidentů evidovaných CSIRT.CZ je poté pravděpodobné (55–70 %), že reálný počet incidentů v ČR se za rok 2022 pohybuje ve vyšších stovkách.**

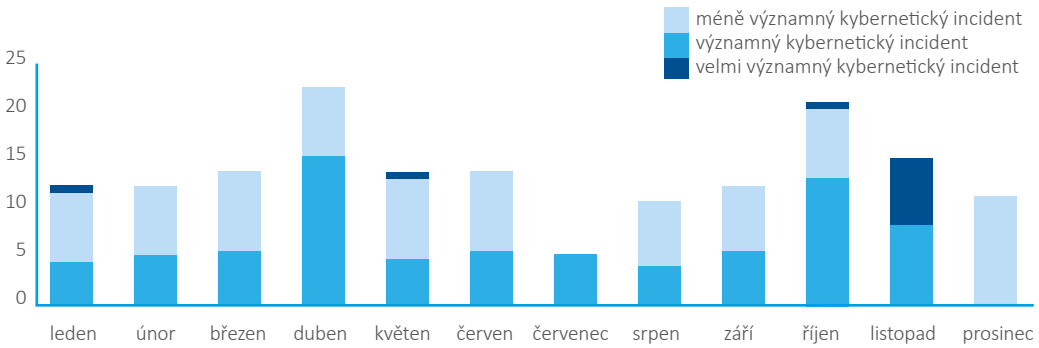
Do zaznamenaných incidentů roku 2022 se do jisté míry promítlo dění spojené s ruskou invazí na Ukrajinu. Nejvíce incidentů bylo evidováno v měsících dubnu a říjnu, což bylo v obou případech dáno významným nárůstem počtu DDoS útoků (viz Graf 2). Za tímto nárůstem stály především útoky ruskojazyčných hacktivistických skupin. Za dubnovou DDoS kampaní stála skupina Killnet, zatímco k části říjnových útoků se přihlásila skupina Anonymous Russia. **Útoky obou skupin přitom téměř jistě (90–100 %) souvisely s českou podporou Ukrajiny.**

[1] Prezentované informace vycházejí ze zdrojů NÚKIB a z vyhodnocení 317 dotazníků (viz část O dokumentu).



Graf 2: Počet řešených incidentů v průběhu roku 2022

Jedním z trendů je již druhým rokem klesající počet zaznamenaných velmi významných kybernetických incidentů. Oproti tomu však narostl počet významných kybernetických incidentů, zatímco počet méně významných kybernetických incidentů se mírně snížil (viz Graf 3). Stejně jako tomu bylo během roku 2021, byl incidenty zdaleka nejvíce zasažen sektor veřejné správy. Ve větším odstupu následoval sektor zdravotnictví a soukromý sektor. **Nově však NÚKIB zaznamenal nárůst incidentů v sektoru dopravy, jehož hodnoty se v předchozích letech pohybovaly pouze v řádu jednotek, zatímco v roce 2022 jich bylo 14**.



Graf 3: Přehled řešených incidentů v roce 2022 podle významnosti

V probíhajícím roce 2023 bude kybernetický prostor v ČR pravděpodobně (55–70 %) do jisté míry i nadále ovlivňován děním na Ukrajině. Ačkoliv se tamní válečný konflikt do dění v českém kyberprostoru v roce 2022 promítl (viz níže), nevedl k výraznějšímu nárůstu závažnějších kybernetických útoků vůči českým subjektům. Takové útoky mířily především na samotnou Ukrajinu, popř. na její geograficky nejbližší spojence. Nelze však vyloučit (25–50 %), že v následujícím období může k takovým útokům docházet také v českém kyberprostoru.

Regulované subjekty	Neregulované subjekty
72 incidentů	**74 incidentů**

Během předchozího roku nadále taktéž pokračoval trend rostoucího počtu incidentů u neregulovaných subjektů. Za rok 2022 jich NÚKIB evidoval 74, oproti 64 během roku 2021. **U regulovaných subjektů naopak došlo meziročně ke snížení počtu kybernetických incidentů.**

Klasifikace kybernetických incidentů nahlášených NÚKIB[2]

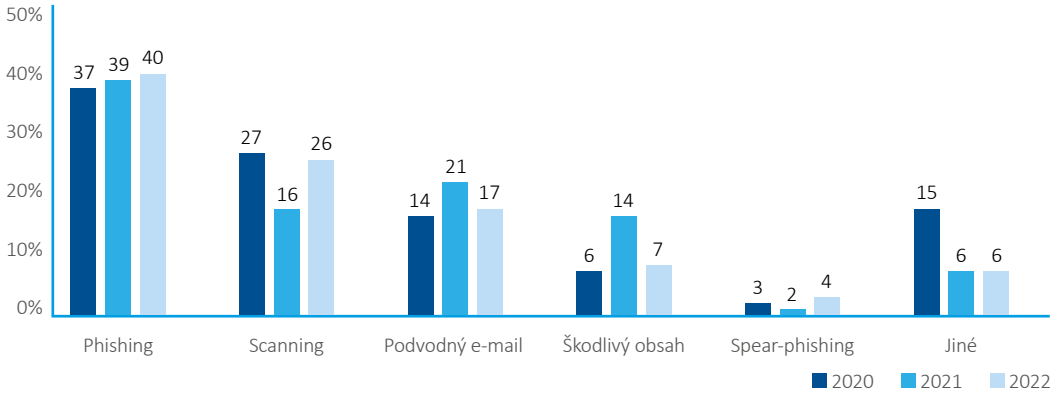
Do klasifikace incidentů se z velké části promítly rozsáhlé vlny DDoS útoků a za uplynulý rok tak převažovaly incidenty cílící na dostupnost. Tyto nicméně nezahrnovaly pouze DDoS útoky, ale v některých případech také prosté technické chyby vedoucí k výpadku systémů. V rámci kategorií dostupnosti a škodlivého kódu zůstává nadále trvalým trendem ransomware, který byl v roce 2022 vyjma října evidován každý měsíc. Jeho počet se však meziročně snížil, což se projevilo celkovým poklesem v kategorii škodlivý kód. K poklesu došlo také v incidentech, které NÚKIB klasifikuje jako průnik. To bylo dáno zejména již zmíněnou absencí kampaní zneužívajících závažných zranitelností, ke kterým docházelo v roce 2021.

	Procentuální zastoupení v incidentech 2021		2022	Vývoj v průběhu roku
Dostupnost např. narušení dostupnosti způsobené DoS/DDoS útokem nebo sabotáží	34 %	↗	**58 %**	
Škodlivý kód např. virus, červ, trojský kůň, dialer, spyware	25 %	↘	**8 %**	
Průnik např. kompromitace aplikace nebo uživatelského účtu	22 %	↘	**12 %**	
Podvod např. phishing, krádež identity nebo neoprávněné využití ICT	10 %	↗	**11 %**	
Informační bezpečnost např. neautorizovaný přístup k datům, neautorizovaná změna informace	8 %	↗	**10 %**	
Pokus o průnik např. pokus o zneužití zranitelnosti, pokus o přihlášení apod.	1 %	↘	**0 %**	
Sběr informací např. skenování, sniffing, sociální inženýrství	0 %	→	**0 %**	
Urážlivý obsah	0 %	→	**0 %**	
Ostatní	0 %	↗	**3 %**	

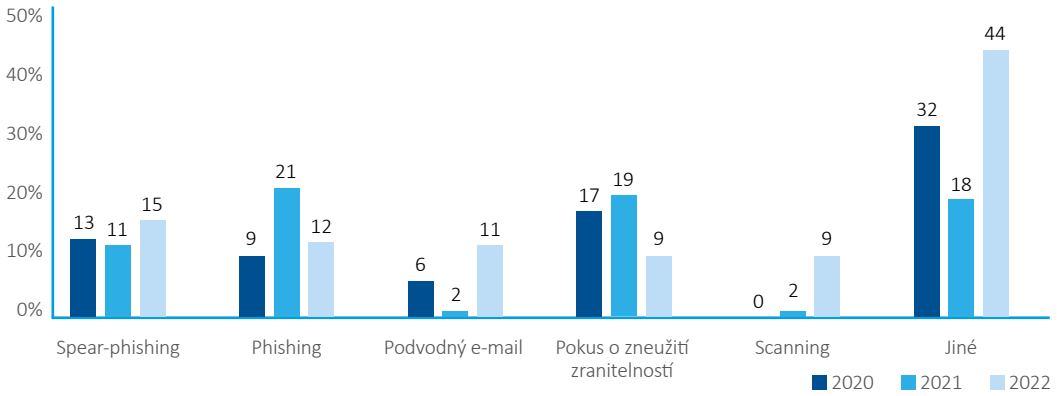
[2] Klasifikace kybernetických incidentů je založena na taxonomii ENISA: Reference Incident Classification Taxonomy — ENISA (europa.eu).

Incidenty pohledem subjektů: rostoucí četnost i větší sofistikovanost phishingu

Mezi nejčastější typy kybernetických útoků, se kterými se dotazované organizace setkaly během roku 2022, patřily phishing, skenování vnější sítě a podvodné e-maily (viz Graf 4). Jedná se o technicky spíše méně náročné a snadno detekovatelné typy útoků, které se v této statistice objevují pravidelně. Změnou oproti minulému roku bylo vnímání závažnosti spear-phishingu, který se stal nejzávažnějším typem útoku podle dotazovaných organizací (viz Graf 5). Tento trend je pravděpodobně (55–70 %) dán rostoucí sofistikovaností a perzistencí útočníků, kteří tyto typy útoků provádí. **Různé formy phishingu a podvodných e-mailů zároveň zůstávají jedním z hlavních vektorů kybernetických útoků také v globálním měřítku.**[3] V celkovém úhrnu zaznamenalo pokus o kybernetický útok během roku 2022 68 % dotazovaných organizací, nicméně k narušení důvěrnosti, integrity nebo dostupnosti informací či služeb došlo pouze u 24 % z nich (viz Graf 6).

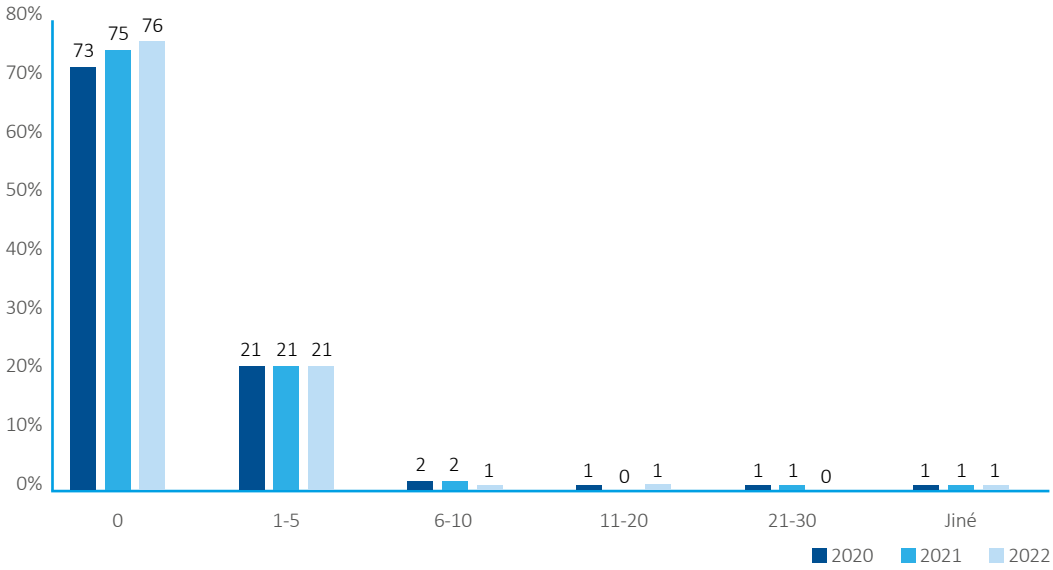


Graf 4: Kategorie nejčastějších typů kybernetických útoků v letech 2020–2022 (% respondentů)



Graf 5: Kategorie nejzávažnějších typů kybernetických útoků v letech 2020–2022 (% respondentů)

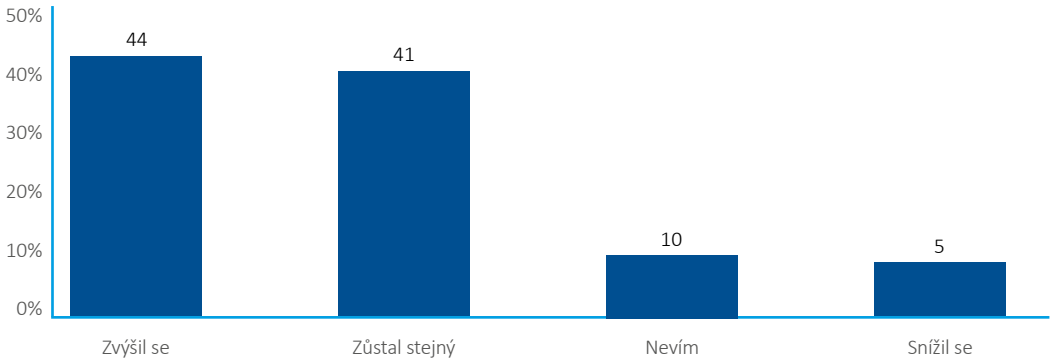
[3] *Microsoft. 2022. Microsoft Digital Defense Report 2022. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us*



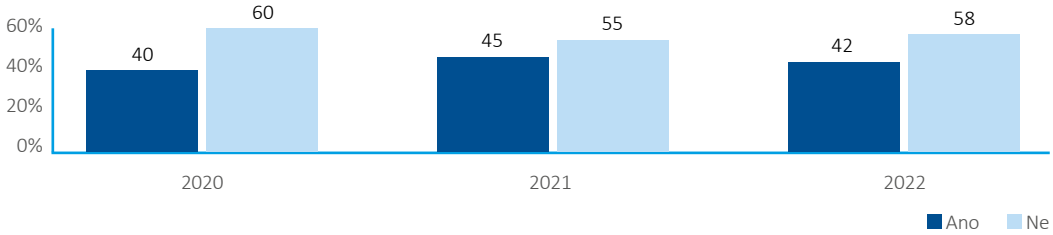
Graf 6: Počet případů narušení důvěrnosti, integrity nebo dostupnosti informací v letech 2020–2022 (% respondentů)

Finance vynaložené na kybernetickou bezpečnost: rostoucí počet organizací navyšujících rozpočty

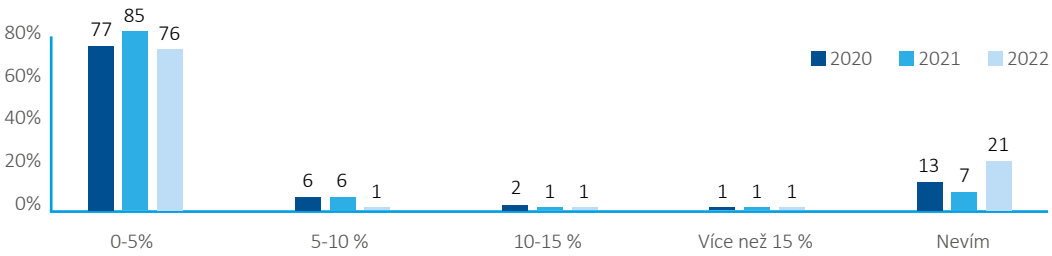
Pozitivním trendem, který započal již během roku 2021, je nadále rostoucí počet organizací, které meziročně navýšily své rozpočty v oblasti zajišťování kybernetické bezpečnosti. Navzdory poměrně složité ekonomické situaci spojené s vysokou inflací či růstem cen energií došlo ke zvýšení rozpočtu alokovaného na zajišťování kybernetické bezpečnosti téměř u poloviny dotazovaných organizací (viz Graf 7). Jedním z důvodů růstu rozpočtů však může být právě inflace, jelikož hodnocení adekvátnosti výše rozpočtu zůstává meziročně bez významnějších změn. **Mírná většina respondentů i nadále hodnotí vynaložené prostředky jako nedostatečné** (viz Graf 8). Obdobně jako v minulých letech vydává většina subjektů na kybernetickou bezpečnost 0–5 % svého rozpočtu (viz Graf 9).



Graf 7: Vývoj rozpočtů respondentů alokovaných na kybernetickou bezpečnost oproti roku 2021 (% respondentů)



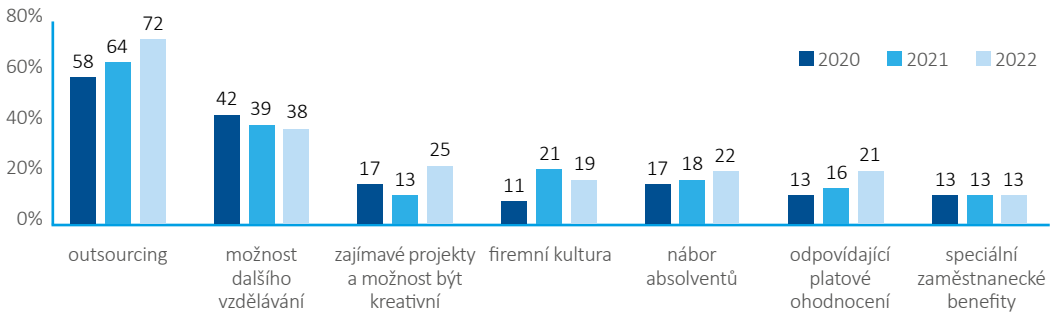
Graf 8: Byly finance alokované na kybernetickou bezpečnost v letech 2020–2022 podle respondentů dostatečné? (% respondentů)



Graf 9: Podíl rozpočtu alokovaného na kybernetickou bezpečnost z celkového rozpočtu organizací v letech 2020–2022 (% respondentů)

Lidé – odborníci: více outsourcingu i nové příležitosti pro absolventy

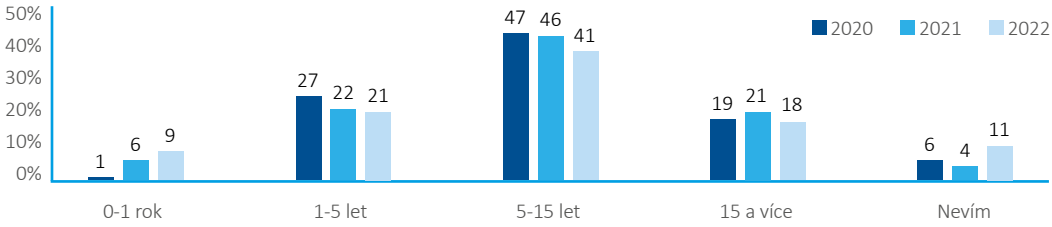
Nedostatek odborníků na kybernetickou bezpečnost zůstal i během roku 2022 jedním z hlavních problémů a výzvou pro české instituce a organizace. S tímto nedostatkem úzce souvisí i vysoké nároky na finanční ohodnocení potenciálních zaměstnanců. **Celkem 74 % respondentů totiž uvedlo, že právě nižší výše finančního ohodnocení je zásadním faktorem odrazujícím uchazeče při náborech na pozice v oblasti kybernetické bezpečnosti**. Dotazované organizace tuto problematiku řeší několika různými způsoby, přičemž během posledních tří let lze identifikovat zejména tři obecnější vzestupné trendy (viz Graf 10). Počet organizací, které nedostatek odborníků v oblasti kybernetické bezpečnosti řeší outsourcingem, vzrostl od roku 2020 o téměř 15 %, přičemž během uplynulého roku toto řešení uplatnily téměř tři čtvrtiny respondentů. Pozvolný nárůst lze identifikovat také v náboru absolventů. Pětina respondentů pak reagovala na nedostatek odborníků i odpovídajícím platovým ohodnocením. **Převládajícím řešením tak dlouhodobě zůstává outsourcing a možnost dalšího vzdělávání.**



Graf 10: Jak se organizace v letech 2020–2022 snažily vypořádat s nedostatkem odborníků v oblasti kybernetické bezpečnosti? (% respondentů)

Meziročně také narostl počet respondentů, jejichž organizace se snaží nabízet odborníkům zajímavější a kreativní prostředí. Větší důraz na nábor absolventů se následně promítl i do odpovědí respondentů na dotaz mapující průměrnou délku relevantní praxe zaměstnanců v oblasti kybernetické bezpečnosti (viz Graf 11).

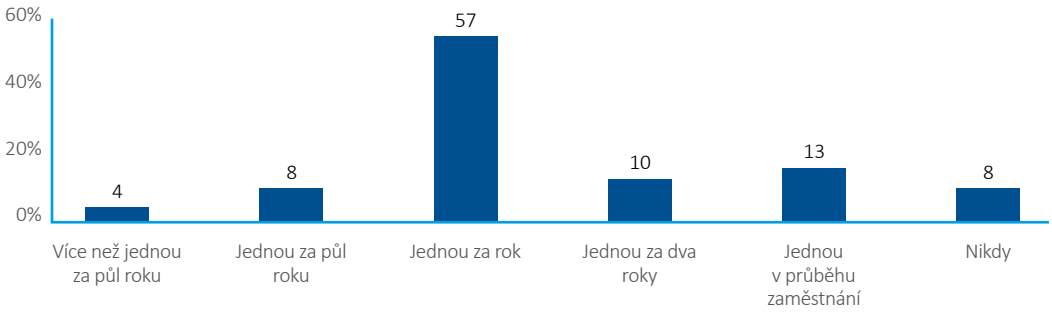
Mezi pět nejobtížněji obsazovaných pozic poté respondenti řadí architekty kybernetické bezpečnosti, správce síťové infrastruktury, pozice bezpečnostního dohledu SIEM, správce serverové infrastruktury a auditory kybernetické bezpečnosti.



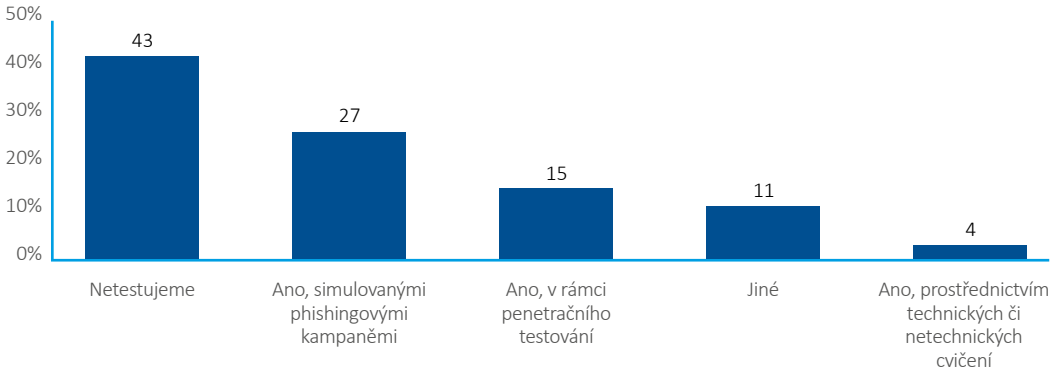
Graf 11: Průměrná relevantní praxe zaměstnanců zajišťujících kybernetickou bezpečnost v organizacích respondentů (% respondentů)

Lidé – uživatelé: většina organizací své uživatele školí i testuje

Jelikož značná část kybernetických incidentů je způsobena chybou či neopatrností uživatelů, jejich vzdělávání a testování představuje neoddělitelnou součást zajišťování kybernetické bezpečnosti. Dobrou zprávou v tomto ohledu je, že pouze necelých 5 % respondentů uvedlo absenci jakéhokoliv školení zaměstnanců v oblasti kybernetické bezpečnosti. Více než polovina dotazovaných organizací proškoluje uživatele alespoň jednou ročně, přičemž téměř desetina organizací se aktivně věnuje školení více než jednou za půl roku (viz Graf 12). **Přes polovinu dotazovaných organizací zároveň své uživatele testuje, nejčastěji cestou simulovaných phishingových kampaní.** Řada organizací dále využívá i techniky penetračního testování či účast na technických i netechnických cvičeních k posílení kybernetické bezpečnosti (viz Graf 13).



Graf 12: Frekvence školení uživatelů v oblasti kybernetické bezpečnosti v organizacích za rok 2022 (% respondentů)



Graf 13: Formy testování odolnosti zaměstnanců proti kybernetickým hrozbám v organizacích za rok 2022 (% respondentů)

Útoky na dostupnost: významný nárůst DDoS útoků ruskojazyčných hacktivistů

Jedním z dopadů ruské invaze na Ukrajinu bylo zvýšené riziko kybernetických útoků vůči státům podporujícím Ukrajinu, na což NÚKIB opakovaně během předešlého roku upozorňoval. Přestože nedošlo k naplnění závažnějších scénářů možných rizik, ČR byla terčem řady kybernetických útoků, které mají téměř jistě (90–100 %) souvislost s tamním konfliktem. **Během roku 2022 totiž v tuzemsku došlo k několika vlnám DDoS útoků, ke kterým se přihlásili ruskojazyční hacktivisté.** Jejich cílem byly primárně subjekty veřejného sektoru, ale i řada soukromých organizací.

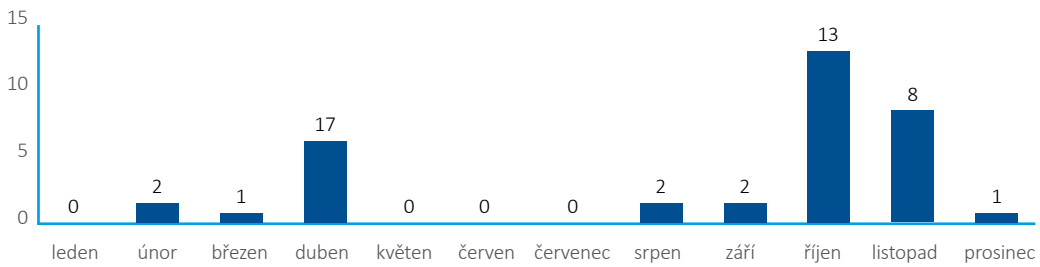
Dubnová DDoS kampaň skupiny Killnet

Během dubna roku 2022 provedla ruskojazyčná hackerská skupina Killnet dvě série DDoS útoků proti webovým stránkám českých subjektů. První vlna probíhala od 19. do 21. dubna, přičemž zasáhla třináct subjektů, včetně NÚKIB a řady ministerstev ČR. Druhá vlna proběhla 27. dubna, kdy útočníci napadli dalších devět subjektů. Počátek útoků se překrýval s oznámením oprav ukrajinské těžké vojenské techniky na území ČR, přičemž útočníci své útoky oznámili na svém telegramovém účtu.

Říjnová DDoS kampaň skupiny Anonymous Russia

Dne 2. října 2022 oznámila hackerská skupina Anonymous Russia na svém telegramovém účtu útoky proti českým subjektům. Mezi uváděnými cíli byly vládní instituce, média, banky či letiště. Reálný dopad útoků byl však omezený a zasažen byl nakonec jen zlomek deklarovaných cílů. V rámci této kampaně se zároveň nepodařilo z vyjádření skupiny prokázat propojení s konkrétním krokem ČR, který by byl pro útok záminkou.

Vedle těchto dvou konkrétních kampaní však docházelo k DDoS útokům i ve zbylých částech roku 2022, přičemž měsíční počet incidentů způsobených DDoS útoky, které byly zároveň řešeny NÚKIB, lze vidět níže (viz Graf 14). **Podle dat respondentů dotazníkového šetření se přitom s pokusem či úspěšným DDoS útokem setkalo během minulého roku 28 % dotazovaných organizací, tudíž počet incidentů nahlášených NÚKIB je téměř jistě (90–100 %) pouze zlomkem reálné četnosti**



Graf 14: Měsíční vývoj DDoS útoků řešených NÚKIB

Přestože DDoS útoky jsou obecně považovány spíše za méně sofistikované, **během uplynulého roku lze identifikovat snahu části útočníků provádět silnější a déletrvající DDoS útoky s cílem odepřít dostupnost služeb po co nejdelší dobu** prostřednictvím obcházení obvyklých mitigačních opatření či využívání více technik DDoS útoků současně. V případě výše zmiňovaných proruských hacktivistických skupin dále DDoS útoky sloužily i jako nástroj propagandy. Navzdory minimálním dopadům byly DDoS útoky v tuzemsku často silně medializovány, přičemž skupiny jako Killnet či Anonymous Russia posléze tyto články přebíraly a propagovaly je svému domácímu publiku na sociální síti Telegram se snahou zveličovat jejich reálné dopady. **Přílišná medializace útoků v napadených zemích tak paradoxně podporovala cíle útočníků.**

Malware jako služba: rostoucí příležitosti pro kyberkriminální aktéry

Další z hrozeb, jejíž rozmach během uplynulého roku NÚKIB zaznamenal, je prodej nástrojů k provádění kybernetických útoků formou služby v tzv. cybercrime-as-a-service modelu (kyberzločin jako služba). Kyberkriminální aktéři nabízejí své služby na černém trhu (zejména skrze internetové stránky v rámci tzv. darkwebu), které si mohou zakoupit aktéři nedisponující dostatečnými technickými znalostmi a prostředky. Konkrétně se může jednat o ransomware či jiné druhy malwaru, přístupy do již kompromitovaných systémů, komplexní služby pro phishingové kampaně nebo například přímé provádění vishingu.

Vishing-as-a-service
Nabízí pronájem hlasových systémů určených pro provádění vishingu.

Access-as-a-service
Nabízí přístup ke kompromitovaným účtům či systémům.

Malware-as-a-service
Nabízí malware k následnému využití v rámci kybernetických útoků.

Phishing-as-a-service
Nabízí komplexní phishingové služby od detailních návodů až po předpřipravené e-maily či legitimně vypadající škodlivé stránky.

DDoS-as-a-service
Nabízí přístup k infikovaným zařízením připojeným k internetu (tzv. botnet) za účelem provádění DDoS útoků.

Cybercrime-as-a-service je tedy obchodním modelem, který umožňuje prakticky komukoliv s dostatečnými finančními prostředky využívat nástroje či služby k provádění kybernetických útoků. Škodlivá kybernetická činnost se tak stává dostupnější, a to i pro relativně nezkušené útočníky. Vzhledem k narůstající popularitě tohoto modelu, který s sebou přináší velké zisky, roste také konkurence, což zpětně vede k širší nabídce produktů, ale i ke snižování ceny. To pak následně činí poskytované služby a nástroje dostupnější širšímu okruhu potenciálních zájemců.

Ransomware-as-a-service

Velmi rychle rozvíjející se hrozbu posléze představuje ransomware-as-a-service (ransomware jako služba). NÚKIB dlouhodobě eviduje ransomwarové útoky, jejichž obětí se stává široké spektrum veřejných i soukromých subjektů. **Od konce roku 2019 přitom začal převažovat trend ransomwaru nabízeného právě ve formě služby.** Ten je specifický svým důrazem na vícenásobné vydírání. Jeho součástí mohou být vyjma tradičního zašifrování též exfiltrace dat a hrozba jejich zveřejněním, DDoS útoky pro zvýšení tlaku na oběť nebo kontaktování zákazníků či partnerů oběti pro další navýšení tlaku z důvodu platby výkupného (viz Obrázek 1).

Obrázek 1: Čtyři úrovně ransomwarového vydírání (Zdroj: NÚKIB)

V České republice přitom NÚKIB během roku 2022 zaznamenal 27 kybernetických incidentů způsobených ransomwarem, přičemž pokus či úspěšný ransomwarový útok v rámci dotazníkového šetření uvedlo 15 % respondentů. **Ransomware, i v podobě služby, tudíž v roce 2022 představoval pokračující trend a hrozbu pro bezpečnost tuzemských organizací.**

Phishing, spear-phishing a vishing: zvyšující se sofistikovanost a perzistence aktérů

Obdobně jako v roce 2021 představoval nejčastější vektor kybernetických útoků phishing, spear phishing a podvodné e-maily. Během minulého roku zároveň pokračoval trend jejich zvyšující se sofistikovanosti. **NÚKIB zaznamenal i více případů vishingu,** tedy podvodných telefonátů, při kterých se útočníci snaží získat přístup do systémů oběti spolu s vylákáním přihlašovacích údajů, zejména do internetového bankovnictví. S pokusem či úspěšným útokem pomocí phishingu se během roku 2022 setkalo 92 % respondentů, se spear-phishingovými e-maily 49 % respondentů, s podvodnými e-maily 89 % respondentů, přičemž vishing zaznamenalo 20 % respondentů. Oproti minulému roku se tedy jedná o mírné zvýšení. Před výskytem těchto typů útoků během minulého roku zároveň NÚKIB několikrát varoval formou upozornění (viz Box).

NÚKIB v reakci na phishingové kampaně vydal v roce 2022 tři upozornění. Dvě z nich reagovala na probíhající vishingovou kampaň během února a dubna. Kampaň měla za cíl přesvědčit oběti o kompromitaci jejich systému, kterou operátor, předstírající příslušnost ke společnosti Microsoft, nabídne vyřešit. Operátor se však pokusí získat přístup k systému oběti skrze nástroj pro vzdálený přístup, jejž využije k získání údajů o platební kartě. Dále oběť navádí k potvrzení dvoufázového ověření zaslaných plateb, případně do systému oběti nainstaluje tzv. keylogger.

- Upozorňujeme na novou vlnu podvodných vishingových telefonátů
- Upozorňujeme na stále trvající kampaň podvodných vishingových telefonátů

Během srpna poté NÚKIB vydal upozornění spojené s phishingovou kampaní zneužívající tematiku sociálních příspěvků na bydlení. Podvodné zprávy se šířily e-mailem či SMS zprávami, které se snažily oběti přimět ke sdílení bankovní identity s útočníky. Kampaň se objevovala po dobu několika týdnů.

- Upozornění na phishingovou kampaň s cílem zneužít bankovní identitu

Nejlepší obranou proti těmto pokusům nadále zůstává osvěta společnosti, tedy informovanost, poučenost a obezřetnost lidí a zlepšování schopností tyto pokusy rozpoznat.

92 %
dotazovaných organizací uvedlo, že na ně byl v roce 2021 veden **phishingový útok** nebo pokus o něj
(+2 % oproti 2021)

89 %
dotazovaných organizací uvedlo, že na ně byl v roce 2021 veden útok nebo pokus o něj formou **podvodného e-mailu**
(+5 % oproti 2021)

49 %
dotazovaných organizací uvedlo, že na ně byl v roce 2021 veden **spear-phishingový útok** nebo pokus o něj
(+2 % oproti 2021)

20 %
dotazovaných organizací uvedlo, že na ně byl v roce 2021 veden **vishingový útok** nebo pokus o něj
(+9 % oproti 2021)

NÚKIB zároveň eviduje trend vzrůstající perzistence útočníků, kteří mnohdy nasazují automatizovanější metody tvorby infrastruktury, aby udrželi kampaň v chodu i v případě proaktivních zásahů. Roste také sofistikovanost útočníků, zejména v oblasti věrohodnosti podvodných e-mailů či falešných webových stránek (více k tomuto tématu v kapitole: Výhled trendů v kybernetické bezpečnosti v ČR na roky 2023 a 2024).

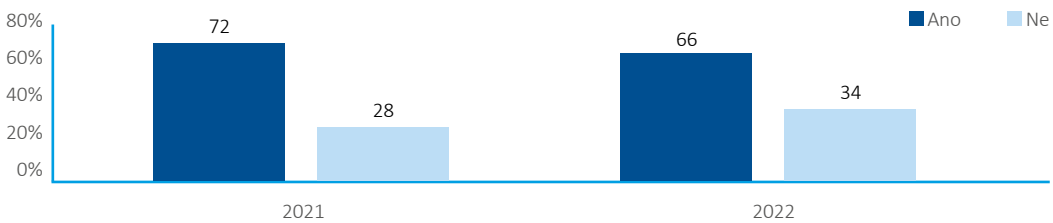
Útoky na dodavatelský řetězec: nízký počet, ale potenciálně vysoké dopady

Útok skrze dodavatele služeb či pokus o něj zaznamenalo v roce 2022 necelých 6 % dotazovaných institucí či organizací. Jedná se o stejnou hodnotu jako v roce 2021, přičemž i nadále patří tento typ útoku mezi nejméně časté. To je pravděpodobně (55–70 %) způsobeno kombinací několika faktorů, a to zejména nižším výskytem tohoto typu útoku v ČR obecně, nízkou schopností detekce ze strany organizací a s tím spjatou snahou útočníků o nepozorovanou přítomnost v systémech oběti.

NÚKIB nicméně během května minulého roku řešil několik závažných případů, které zdůrazňují potřebu procesu řízení dodavatelů. V jednom z kybernetických incidentů, který napadené organizaci způsobil značné škody, se útočník dostal do sítě své oběti skrze kompromitovaný VPN účet její servisní firmy. Na další dva případy špatného zabezpečení přišly organizace samy, pravděpodobně (55–70 %) ještě před tím, než slabého místa stačili zneužít útočníci. Tyto organizace zjistily, že dodavatel informačního systému jejich citlivá data ukládá na webové uložiště bez potřeby autentizace.

Řízení dodavatelů je jedním z organizačních bezpečnostních opatření, k jejichž provádění jsou povinny vybrané osoby spadající do působnosti zákona o kybernetické bezpečnosti. Proces řízení dodavatelů slouží především k identifikaci rizik spojených s využíváním služeb třetích stran a jejich následné mitigaci.

V rámci meziročního srovnání počtu respondentů, jejichž organizace řídí rizika spojená s dodavateli, lze identifikovat mírný pokles (viz Graf 15). V rámci kritické informační infrastruktury (dále jen „KII“) tato rizika řídí 86 % dotazovaných organizací.



Graf 15: Řídí Vaše organizace rizika spojená s dodavateli? (meziroční srovnání, % respondentů)

NÚKIB zároveň během roku 2022 na základě pověření Bezpečnostní rady státu pracoval na návrhu zákona, který má za cíl významně omezit vliv rizikových dodavatelů na nejvýznamnější infrastrukturu ČR. Hrozby v oblasti kybernetické bezpečnosti plynoucí z dodavatelských řetězců technologií jsou sice již dlouhodobě známy, dosud však v právním řádu ČR neexistuje komplexní právní řešení umožňující rizika plynoucí z těchto hrozeb cíleně vyhodnocovat a snižovat (více v kapitole: Národní úroveň kybernetické bezpečnosti: pokračující posilování odolnosti vůči kybernetickým hrozbám).

Aktéři kybernetických hrozeb

Aktivity státem podporovaných aktérů v kybernetickém prostoru a kyberkriminalita dlouhodobě patří mezi nejvážnější hrozby pro kybernetickou bezpečnost ČR.

Státem podporované skupiny jsou zpravidla vysoce sofistikovanými aktéry, kteří k dosažení svých cílů využívají širokou škálu technik a neustále zdokonalují své nástroje. Zvýšené riziko poté během uplynulého roku představovali pro ČR zejména ruští státní aktéři. **V kontextu ruské invaze na Ukrajinu došlo počátkem roku 2022 ke kybernetickému útoku, který byl na základě** koordinované atribuce **všech členských států EU přisouzen Ruské federaci. Tento útok měl nepřímé dopady i na tuzemské subjekty (viz Box).**

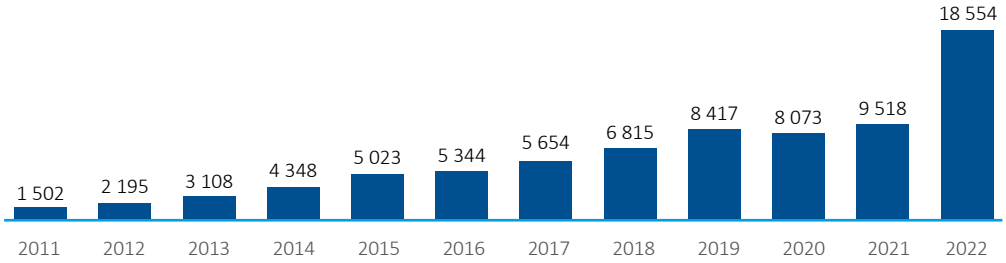
Kybernetický útok na poskytovatele satelitního internetového připojení Viasat

V brzkých ranních hodinách 24. února 2022, takřka souběžně s invazí ruských ozbrojených sil, došlo ke kybernetickému útoku vůči pozemním terminálům společnosti Viasat zajišťujícím satelitní internetové připojení na území Ukrajiny. Jeho následky postupně omezily jejich funkcionalitu, přičemž následně došlo k přelití (tzv. spilloveru) těchto následků i na desetitisíce dalších uživatelů v severní Africe, na Blízkém východě a v Evropě, včetně uživatelů v ČR. Díky relativně nízkému počtu uživatelů této služby nedošlo v ČR k významnějším dopadům útoku.

NÚKIB během roku 2022 zaznamenal také kyberšpionážní kampaň vůči jedné ze strategických institucí státu, za kterou velmi pravděpodobně (75–85 %) stojí ruským státem sponzorovaný aktér APT29 (označován též jako Cozy Bear, The Dukes či NOBELIUM). **Ten je obvykle připisován ruské Službě vnější rozvědky (SVR).** V rámci této kampaně došlo ke kompromitaci e-mailové schránky jednoho ze zaměstnanců cílové instituce, kterou útočník následně využil k rozesílání spear-phishingových e-mailů na více než tisícovku adres partnerských organizací. Dalším krokem byla snaha útočníka kompromitovat i další zaměstnance napadené instituce, přičemž maximálně využíval informace obsažené v původní kompromitované schránce. **Seznam obětí kampaně indikuje motivaci aktéra získat přístup k informacím strategické povahy.**

NÚKIB během uplynulého roku taktéž evidoval zvýšenou aktivitu proruských hacktivistických uskupení Killnet či Anonymous Russia, která byla zodpovědná za DDoS útoky vůči řadě českých subjektů. Tyto skupiny však představují spíše méně sofistikované aktéry a dopady jejich útoků byly marginální.

Obecně pak během minulého roku pokračoval rostoucí trend kyberkriminality. Za rok 2022 bylo, podle dat Policie ČR, registrováno celkem 18 554 skutků spadajících do kategorie kybernetické kriminality a ostatní kriminality páchané v kyberprostoru, což značí velmi významný meziroční nárůst o 95 %. Potvrzuje se tím předpoklad, že kyberkriminalita je kontinuálně rostoucí hrozbou, přičemž její další růst je pravděpodobný (55–70 %) i v následujících letech (viz Graf 16).[4]



Graf 16: Vyšetřované kyberkriminální případy v ČR mezi lety 2011 až 2022

[4] *Policie České republiky. 2022. Vývoj registrované kriminality v roce 2022. https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx*

CÍLE KYBERNETICKÝCH ÚTOKŮ

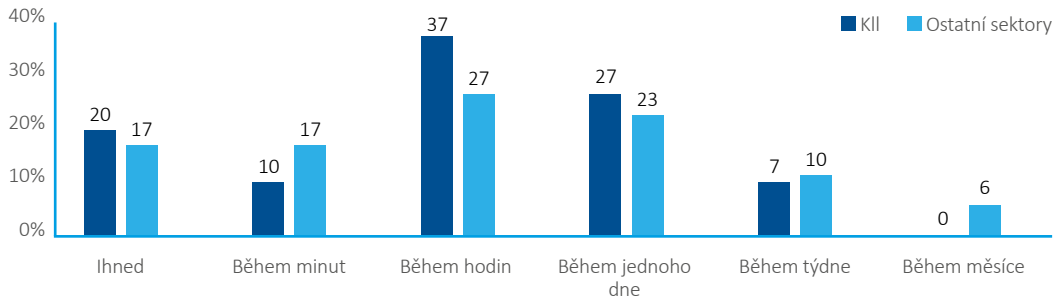
Kritická informační infrastruktura: nárůst útoků na dostupnost služeb

Podobně jako v minulých letech byly subjekty KII v roce 2022 vystaveny pokusům o kybernetický útok. **Počet incidentů registrovaných NÚKIB v dané kategorii se meziročně téměř zdvojnásobil.** Jedná se o významný nárůst, který byl pravděpodobně (55–70 %) způsoben nárůstem DDoS či jiných útoků na dostupnost služeb, které v této kategorii tvořily většinu evidovaných incidentů. Podíl incidentů, které vyústily v omezení dostupnosti služeb, zůstal meziročně takřka stejný, nicméně nominálně jejich počet vzrostl přibližně o 70 %. **Dostupnost je u KII jedním z klíčových prvků, jehož narušení může mít zásadní dopady (viz Box).**

KII je podle § 2 písm. b) zákona o kybernetické bezpečnosti prvek nebo systém prvků kritické infrastruktury v odvětví komunikačních a informačních systémů v oblasti kybernetické bezpečnosti. Kritická infrastruktura samotná je podle § 2 písm. g) zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů, definována jako prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, jejichž narušení by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.

Mezi typické prvky kritické infrastruktury patří elektrárny, přehrady, letiště nebo telekomunikační sítě, ale také strategické finanční instituce nebo státní úřady. **Vyřazení některého z těchto prvků může ochromit poskytování kritických služeb (např. dodávky elektřiny, tepla, vody nebo výplaty důchodů) a v krajním případě způsobit fyzické škody v případě cílené kybernetické sabotáže.**

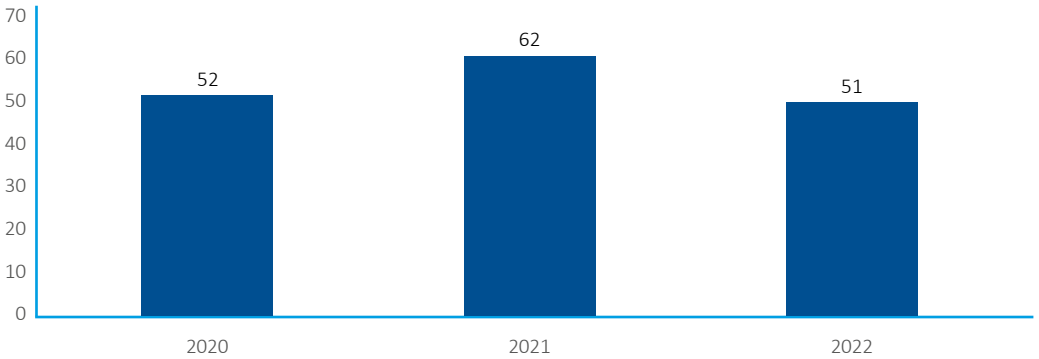
Dobrou zprávou v tomto ohledu je, že meziročně došlo v rámci KII ke zlepšení v rychlosti řešení incidentů, a to navzdory růstu počtu útoků. **Plnou funkcionalitu napadených systémů se podařilo obnovit v horizontu hodin u dvou třetin incidentů, přičemž řešení žádného incidentu netrvalo déle než jeden týden** (viz Graf 17).



Graf 17: Průměrný čas od identifikace kybernetického incidentu až po jeho vyřešení (% incidentů)

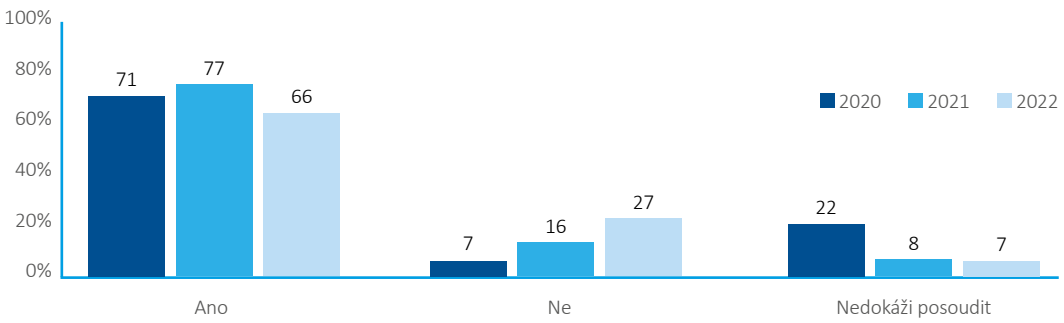
Veřejný sektor: snížení počtu incidentů na hodnoty roku 2020

Veřejný sektor se tradičně řadí k těm nejvíce zasaženým sektorům, přičemž ani během roku 2022 tomu nebylo jinak. **V tomto sektoru je evidováno celkem 51 kybernetických incidentů, což tvoří více než třetinu jejich celkového počtu.** Oproti minulému roku však nominální i proporční zastoupení incidentů mírně kleslo (viz Graf 18). **Největší počet kybernetických útoků směřoval na dostupnost dat, což lze alespoň částečně vysvětlit několika DDoS kampaněmi, které vesměs prováděli mj. ruskojazyční hacktivisté ve spojitosti s českou podporou Ukrajině.** Tyto útoky často cílily právě na různé vládní či veřejné instituce, avšak byly spíše méně sofistikované a velmi limitované v reálných dopadech.



Graf 18: Vývoj počtu incidentů ve veřejném sektoru evidovaných NÚKIB v letech 2020–2022

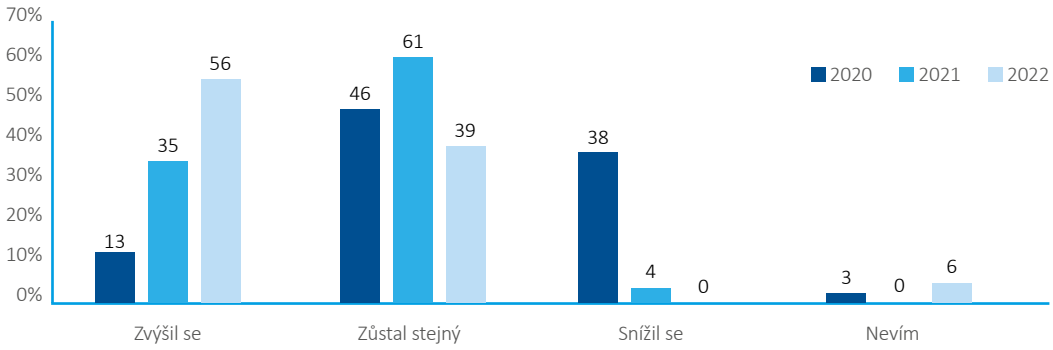
Navzdory meziročnímu snížení počtu incidentů však došlo ke zvýšení počtu respondentů veřejného sektoru, kteří vnímají úroveň zajištění kybernetické bezpečnosti jako nedostatečnou (viz Graf 19). Více než desetiprocentní nárůst respondentů negativně hodnotících úroveň kybernetické bezpečnosti může do určité míry souviset s faktem, že 7 % respondentů v rámci veřejného sektoru zároveň uvedlo, že v jejich organizaci došlo ke snížení rozpočtu na kybernetickou bezpečnost. Dalším faktorem může být i povaha dopadů bezpečnostních incidentů v rámci veřejného sektoru, kdy například necelá pětina subjektů kritické infrastruktury zmínila reputační poškození či omezení dostupnosti služeb, které představují pro tuto skupinu subjektů závažné dopady.



Graf 19: Vnímáte úroveň zajištění kybernetické bezpečnosti ve Vaší organizaci jako dostatečnou? (% srovnání let 2020–2022)

Finanční sektor: zdvojnásobení kybernetických incidentů

Počet kybernetických incidentů v rámci českého finančního sektoru se meziročně zdvojnásobil. Za rok 2021 evidoval NÚKIB pouhé čtyři incidenty, kdežto během minulého roku bylo zaznamenáno osm incidentů. Tři z tohoto počtu poté spadají do kategorie významných incidentů. Z dotazníkového šetření dále vyplývá, že více než polovina respondentů finančního sektoru se během roku 2022 setkala s více než pěti pokusy o kybernetický útok, nicméně většina těchto pokusů nevyústila v kybernetický incident. **Více než polovina respondentů finančních institucí zároveň uvedla, že jejich organizace meziročně zvýšila rozpočet alokovaný na kybernetickou bezpečnost, což v kontextu vývoje posledních let indikuje ochotu do této oblasti kontinuálně investovat a vylepšovat tak úroveň zabezpečení (viz Graf 20).**



Graf 20: Jak se změnil rozpočet Vaší organizace na rok 2022 alokovaný na kybernetickou bezpečnost oproti roku předchozímu? (% srovnání let 2020–2022)

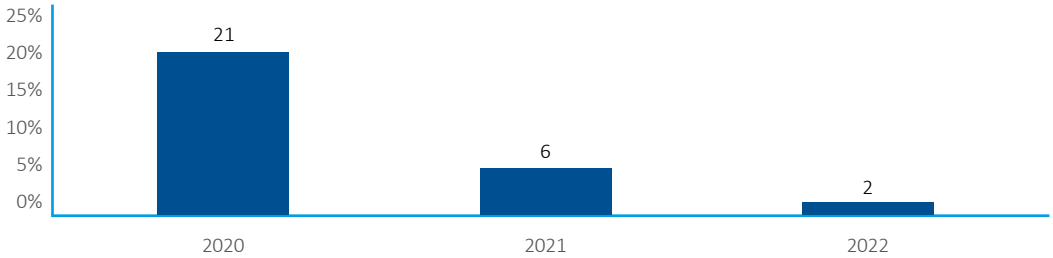
Kromě nárůstu výše popsaných incidentů taktéž meziročně došlo k růstu kybernetických útoků či jiných různých forem internetových podvodů vůči klientům finančních institucí. **Podle dat České bankovní asociace došlo k více než ke zdvojnásobení kybernetických útoků vůči klientům českých bank, přičemž jako hlavní hrozba byl označen především vishing.**[5] NÚKIB v průběhu roku vydal několik varování spojených jak s vishingem, tak i s dalšími podvodnými kampaněmi, které využívají kybernetických nástrojů.[6]

Reakcí na tuto problematiku byl i projekt České bankovní asociace, která ve spolupráci s NÚKIB a dalšími partnery připravila osvětovou kampaň #nePINDej!. Ta je propojena s webovými stránkami Kybertest.cz a má za cíl zvýšení odolnosti občanů ČR proti nejčastějším podvodům spojeným s internetovým bankovnictvím.

[5] *Česká bankovní asociace. 2022. Kybernetických útoků dramaticky přibývá a jsou stále rafinovanější. ČBA proto spouští celonárodní vzdělávací kampaň #nePINdej!. https://cbaonline.cz/kybertest-2022*
[6] *NÚKIB. 2022. Hrozby a zranitelnosti. https://www.nukib.cz/cs/infoservis/hrozby/#1*

Průmysl a energetika: nová rizika spojená s chytrými elektroměry

Energetický sektor čelil během uplynulého roku zásadním výzvám spojeným s dopady ruské invaze na Ukrajinu a následným sankčním režimem či růstem cen energetických surovin. Ke zhoršení situace došlo i v rámci kybernetických incidentů řešených NÚKIB. **Oproti roku 2021 totiž vzrostl počet evidovaných incidentů ze tří na devět, přičemž většinu z nich tvořily útoky cílené na dostupnost služeb či informací.** Naopak podíl ransomwarových útoků, které představovaly významnou hrozbu v minulých dvou letech, se v rámci energetického a průmyslového sektoru snížil (viz Graf 21).



Graf 21: Meziroční srovnání zaznamenaných ransomwarových útoků či pokusů o ně v rámci průmyslového a energetického sektoru (%)

Rok 2022 přinesl i nová rizika v kontextu bezpečnosti dodavatelského řetězce, zejména pro energetická, ale i další průmyslová odvětví, a to v podobě debaty ohledně bezpečnosti nákupu a využívání tzv. smartmeterů (viz Box). Rozmach těchto komponentů, které podle platné legislativy musí být do roku 2027 nasazeny na odběrných místech se spotřebou nad 6 MWh, totiž znamená potřebu zohlednit i jejich kybernetickou bezpečnost. **Hlavní výzvou v tomto směru je právě zajištění bezpečnosti dodavatelského řetězce, jelikož v budoucích letech bude v ČR instalováno velké množství těchto chytrých elektroměrů, které budou výhledově tvořit značnou část energetické distribuční soustavy.**

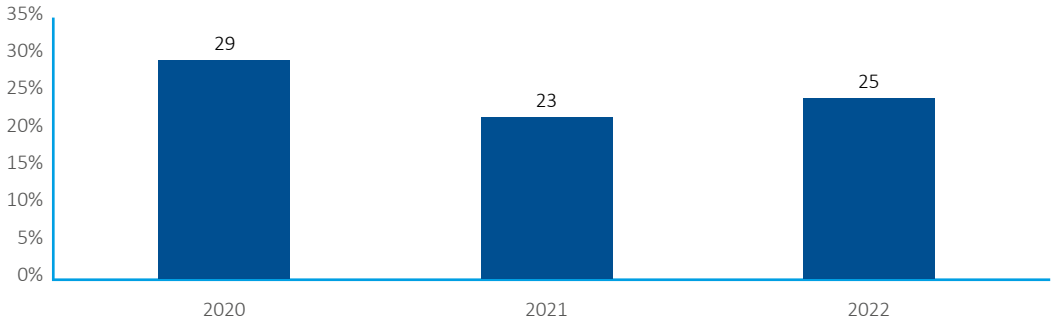
Chytré elektroměry (smartmetery)

Chytré elektroměry jsou v současnosti poměrně dynamicky se rozmáhajícím prvkem digitalizace energetických distribučních sítí. Představují základní prvek inteligentních sítí (tzv. smart grid), přičemž jejich hlavním účelem je zajistit aktuální informace o zatížení soustavy, zajištění lepší kontroly, bezpečnosti a stability rozvodných sítí, ale také zpětnou vazbu o spotřebě energie koncovým zákazníkům. Kromě těchto přínosů však chytré elektroměry představují i určité riziko, neboť se jedná o relativně jednoduchá zařízení připojená k internetové síti. Mohou být tudíž terčem celé řady kybernetických útoků, jejichž dopady mohou být nejen úniky citlivých dat, ale v krajním případě i fyzické poškození distribuční sítě v případě nesprávné manipulace jejich činnosti.

Potenciální riziko kompromitace dodavatelského řetězce lze poté spatřit zejména u společností, které sídlí ve státech, jejichž politicko-právní prostředí zavazuje tyto společnosti spolupracovat s tamními bezpečnostními nebo státními orgány na úkor soukromí či bezpečnosti zákazníků dané společnosti. Hrozbu však představují i společnosti, které skrze vlastnickou strukturu či obchodní spolupráci fakticky tvoří mezičlánek dodavatelského řetězce mezi ČR a zeměmi s výše popsaným rizikovým politicko-právním zázemím. **NÚKIB obě tato rizika v současnosti eviduje, přičemž na to během roku 2022 upozornil prostřednictvím** varování **pro tuzemské subjekty.**

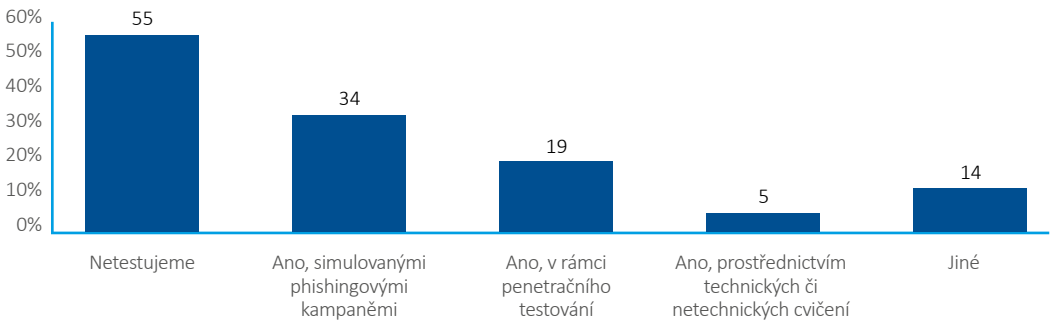
Zdravotnictví: ransomware zůstává relevantní hrozbou

Počet evidovaných incidentů v rámci zdravotnického sektoru se meziročně mírně zvýšil o tři, na výsledných 29 incidentů. NÚKIB zároveň ve zdravotnictví eviduje větší počet méně významných incidentů a padesátiprocentní snížení v kategorii významných a velmi významných incidentů. Podle respondentů však meziročně došlo k mírnému zvýšení počtu organizací, které zaznamenaly pokus o ransomwarový útok, a to o dva procentní body. **Ransomware tak i po konci pandemie covidu-19 zůstává relevantní hrozbou pro čtvrtinu zdravotnických organizací** (viz Graf 22).



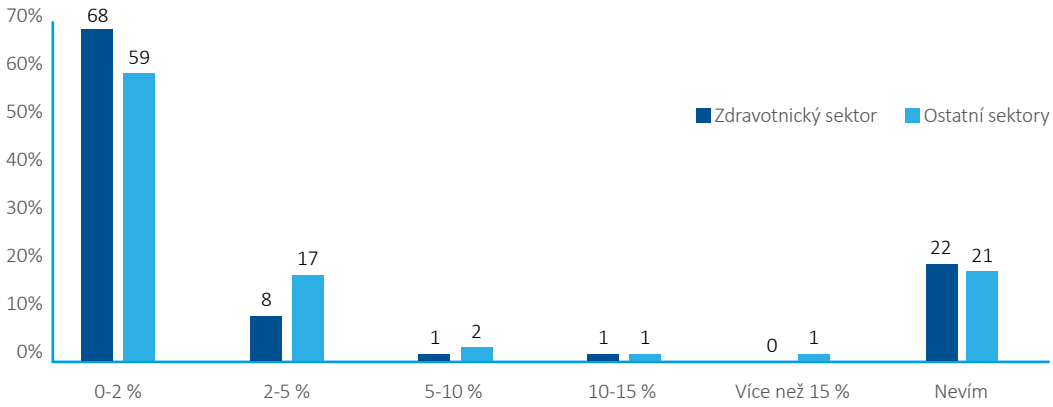
Graf 22: Podíl respondentů zdravotnického sektoru, jejichž organizace zaznamenaly pokus o ransomwarový útok (% srovnání let 2020–2022)

Z hlediska hodnocení závažnosti různých druhů kybernetických útoků byl pak ransomware vnímán respondenty ze zdravotnického sektoru jako méně závažný než phishingové a spear-phishingové útoky či podvodné e-maily, které zároveň představovaly většinu zaznamenaných útoků. **Navzdory vnímání závažnosti a samotné četnosti těchto útoků však simulovanými phishingovými kampaněmi testuje odolnost svých uživatelů pouze třetina respondentů zdravotnického sektoru, přičemž více než polovina respondentů netestuje vlastní uživatele vůbec** (viz Graf 23).



Graf 23: Testujete odolnost Vašich zaměstnanců proti kybernetickým hrozbám? (% respondentů)

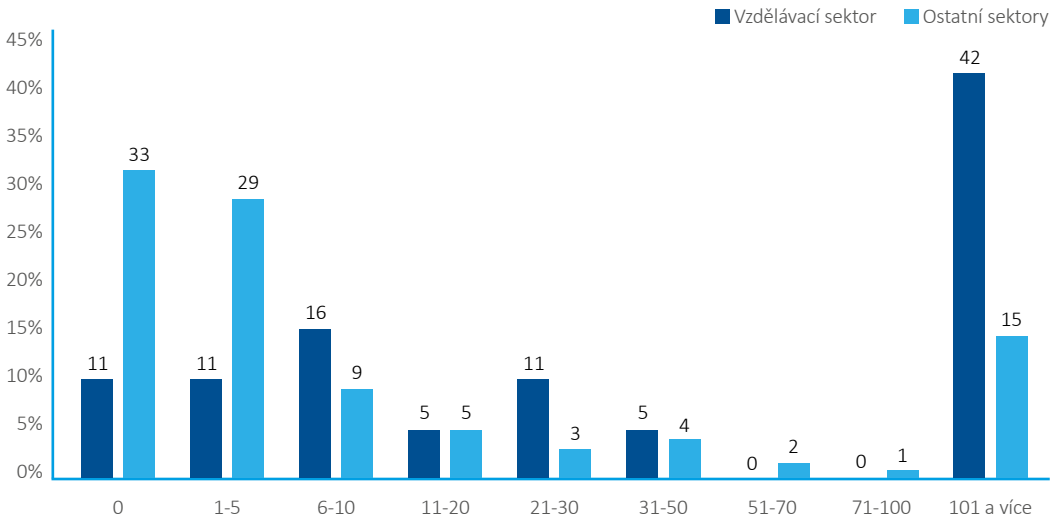
Na tomto stavu se pravděpodobně (55–70 %) podepisuje dlouhodobě neuspokojivá finanční situace těchto subjektů z pohledu alokovaných financí na zajištění kybernetické bezpečnosti, kdy více než 70 % respondentů hodnotí výši rozpočtu v této oblasti jako nedostatečnou. Situaci lze dále demonstrovat na podílu rozpočtu alokovaného na kybernetickou bezpečnost oproti ostatním sektorům, který je v rámci zdravotnictví nižší než průměr ostatních sektorů (viz Graf 24).



Graf 24: Jaké procento z celkového konečného rozpočtu Vaší organizace směřovalo v roce 2022 do nákladů na kybernetickou bezpečnost? (%)

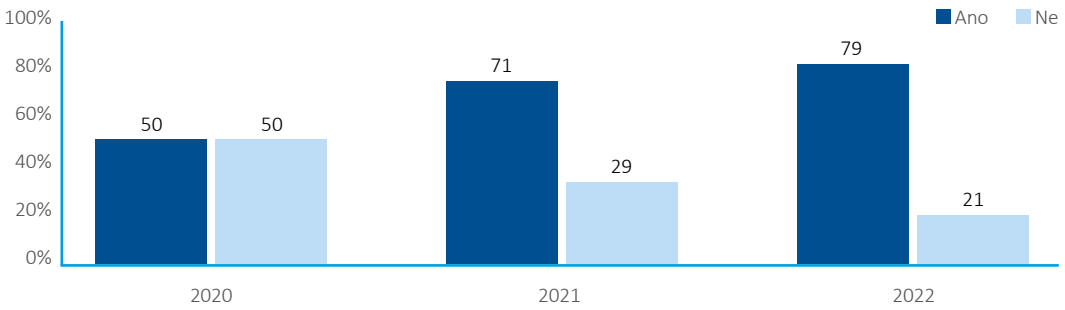
Vzdělávání: rostoucí důraz na školení uživatelů

Vzdělávací sektor, ve kterém NÚKIB během roku 2021 zaznamenal bezprecedentní nárůst kybernetických incidentů, zůstal i během uplynulého roku pro útočníky atraktivním cílem. Přestože počet nahlášených incidentů meziročně klesl na úroveň devíti incidentů, **respondenti ze vzdělávacího sektoru uváděli poměrně vysoké počty pokusů o kybernetické útoky oproti ostatním sektorům.** Největší rozdíly lze sledovat zejména v krajních hodnotách škály, kdy pouze desetina subjektů nezaznamenala žádný pokus o kybernetický útok, přičemž více než dvě pětiny dotazovaných subjektů uvedly 101 a více pokusů (viz Graf 25).



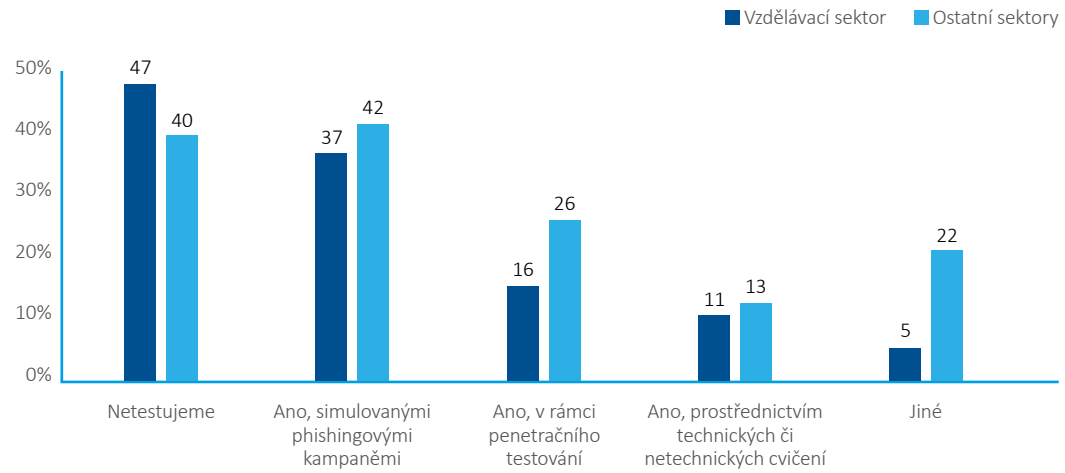
Graf 25: Srovnání zaznamenaných kybernetických útoků či pokusů o ně v roce 2022 (% respondentů)

I během uplynulého roku pokračoval trend phishingových kampaní, kdy phishing a podvodné e-maily tvořily téměř dvě třetiny nejčastějších pokusů o kybernetický útok ve vzdělávacím sektoru. Respondenti nicméně dále uvedli, že přibližně dvě třetiny těchto pokusů nevyústily v kybernetický incident, což je srovnatelná hodnota s ostatními sektory. Jelikož phishingové útoky cílí především na jednotlivé uživatele, tak je obecně za nejlepší prevenci považováno právě jejich školení či testování odolnosti. Pozitivním trendem je setrvalý růst počtu vzdělávacích institucí, které tato školení provádějí (viz Graf 26).



Graf 26: Vývoj organizací vzdělávacího sektoru školící své uživatele v kontextu kybernetické bezpečnosti (%)

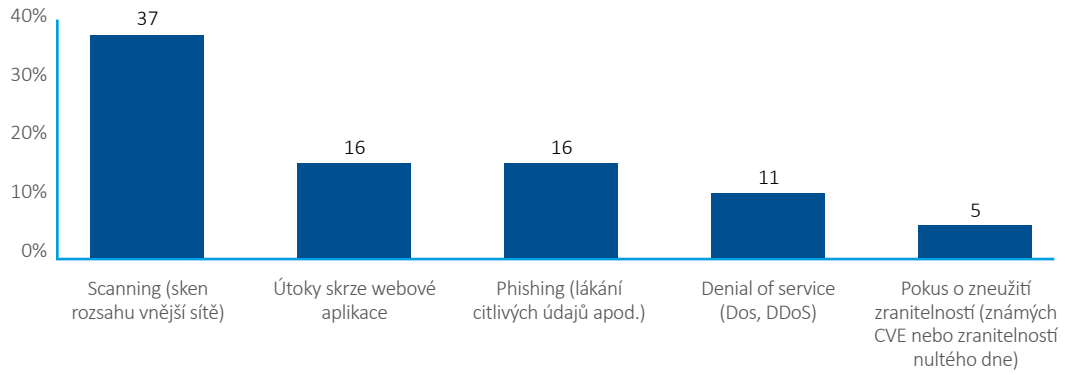
Akademický výzkum zároveň představuje hodnotný cíl pro státem sponzorované skupiny, přičemž phishing může být právě jedním ze způsobů, jakým tito aktéři získávají přístup do systémů oběti. Ke snížení tohoto rizika může přispět mj. i testování odolnosti uživatelů pomocí simulovaných phishingových kampaní. Navzdory rostoucímu podílu organizací ve vzdělávacím sektoru, které své zaměstnance školí, však tento sektor vůči ostatním v rámci testování odolnosti mírně zaostává (viz Graf 27). Nelze vyloučit (25–50 %), že k tomuto stavu přispívá i stav financí alokovaných na kybernetickou bezpečnost, který 84 % respondentů vzdělávacího sektoru hodnotí jako nedostatečný, což je přibližně o pětinu více než u ostatních sektorů.



Graf 27: Testujete odolnost Vašich zaměstnanců proti kybernetickým hrozbám? (% respondentů)

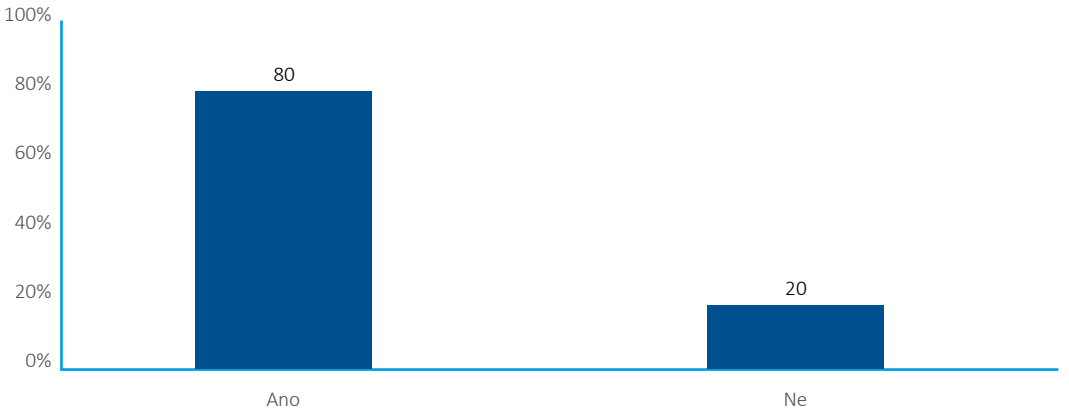
Digitální služby: zacílení širokou paletou útoků

V rámci českého sektoru digitálních služeb (telekomunikace, digitální infrastruktura, internetové služby apod.) evidoval NÚKIB v průběhu roku 2022 celkem osm incidentů. Většina z nich cílila na dostupnost služeb či dat. Z pohledu respondentů bylo nejčastějším typem pokusu o kybernetický útok zejména skenování vnějších portů sítě (tzv. scanning). Oproti ostatním sektorům dosáhl scanning relativně vysokého skóre četnosti, což lze do jisté míry vysvětlit povahou činnosti subjektů v digitálním sektoru. Jelikož poskytují digitální služby, jako je například internetové připojení apod., tak převážně automatické a masivní skenování vnějšího rozsahu sítě útočníky zachytí právě tito poskytovatelé. **Další časté typy útoků poté představovaly útoky skrze webové aplikace, phishing, DoS a DDoS útoky či pokusy o zneužití zranitelností** (viz Graf 28).



Graf 28: Nejčastější typy zaznamenaných kybernetických útoků v sektoru digitálních služeb (% respondentů)

Oproti předešlému roku klesl podíl respondentů, jejichž organizace řídí bezpečnostní rizika spjatá s dodavateli. Činí tak 80 % dotazovaných respondentů, přičemž většina těchto subjektů zohledňuje technická i netechnická rizika v souladu s doporučením NÚKIB pro hodnocení důvěryhodnosti dodavatelů technologií 5G sítí v České republice (viz Graf 29).



Graf 29: Řídíte bezpečnostní rizika spjatá s dodavateli? (% respondentů)

OPATŘENÍ: ČASOVÁ OSA VYBRANÝCH VAROVÁNÍ A UPOZORNĚNÍ NÚKIB V ROCE 2022

LEDEN

Upozornění na zvýšené riziko kyberšpionážních či ransomwarových útoků proti ČR

Během ledna došlo v kontextu rostoucího napětí ve východní Evropě k vydání upozornění na zvýšené riziko kyberšpionáží či ransomwarových útoků vůči českým subjektům. Nejvyšší riziko platilo pro státní instituce, média a KII, přičemž upozornění obsahovalo i přehled konkrétních hrozeb a mitigační či detekční opatření.

ÚNOR

Varování před hrozbou kybernetických útoků na strategické organizace v ČR

Koncem února vydal NÚKIB varování před hrozbou kybernetických útoků na strategické organizace v ČR v kontextu zahájení ruské invaze na Ukrajině. Součástí varování bylo doporučení zvýšené ostražitosti vůči nejčastěji používaným technikám útoků v kyberprostoru, provedení aktualizací informačních systémů a jejich komponent spolu se sadou doporučení v kontextu hrozících DDoS útoků.

KVĚTEN

Varování před použitím chytrých elektroměrů ze zemí s nedůvěryhodným právním prostředím

K dalšímu varování vedla hrozba v kontextu bezpečnosti dodavatelského řetězce spojená s instalací chytrých elektroměrů do tuzemských distribučních soustav. Hrozba spočívá v použití technologie smartmeteringu ze zemí s nedůvěryhodným právním prostředím, které mohou eventuálně způsobit zásadní narušení spolehlivého provozu přenosové soustavy, a to i s možným přeshraničním dopadem.

SRPEN

Upozornění na sadu zranitelností týkající se softwaru VMware

Během srpna NÚKIB vydal upozornění spojené s objevením zranitelnosti softwaru VMware, která útočníkům potenciálně umožňuje získat administrativní přístup do systémů oběti bez nutnosti autentizace. Součástí upozornění bylo doporučení k provedení bezodkladné aktualizace zasažených komponent spolu s jejich seznamem.

ZÁŘÍ

Upozornění na zranitelnosti Microsoft Exchange Server

V září došlo k odhalení dvou zranitelností (CVE-2022-41040 a CVE-2022-41082) široce používaného softwaru Microsoft Exchange Server. NÚKIB v tomto kontextu vydal upozornění spolu s mitigačními opatřeními a indikátory kompromitace.

LISTOPAD

Upozornění na zvýšené riziko DDoS útoků

Koncem roku vydal NÚKIB upozornění v kontextu zvýšeného rizika DDoS útoků, jejichž výskyt se v tomto období zvýšil, pravděpodobně (55–70 %) kvůli společnému zasedání vlád ČR a Ukrajiny. Přestože evidované DDoS útoky během roku 2022 měly krátkodobé a marginální dopady, obecně mohou způsobit i výpadky kritických služeb, jako jsou například portály veřejné správy. Za podstatnou částí těchto útoků stály zejména ruskojazyčné hacktivistické skupiny.

NÁRODNÍ ÚROVEŇ KYBERNETICKÉ BEZPEČNOSTI: POSILOVÁNÍ ODOLNOSTI VŮČI KYBERNETICKÝM HROZBÁM

Při zajišťování kybernetické bezpečnosti na národní úrovni je zásadní spolupráce dotčených subjektů, a to i v rovině nastavování strategického rámce. V roce 2022 došlo k vývoji u několika důležitých aktivit.

Projekt BIVOJ

Smyslem projektu BIVOJ *(**B**ezpečný, **I**novativní, pro **V**eřejnou správu, **O**dolný, **J**ednotný)* je zajistit centrální správu a řízení bezpečnosti sdílených informačních a komunikačních systémů a služeb u organizací ve veřejném sektoru ČR. **Výsledné řešení má umožnit efektivnější dohled, komunikaci a aplikaci bezpečnostních standardů. Díky tomu by tak došlo k navýšení odolnosti veřejného sektoru jako celku a k plošnému zvýšení úrovně kybernetické bezpečnosti.** Projekt je tvořen z několika propojených komponent, které momentálně koordinuje NÚKIB ve spolupráci s dalšími institucemi, např. Vojenským zpravodajstvím či Ministerstvem vnitra ČR.

Koordinované zveřejňování zranitelností

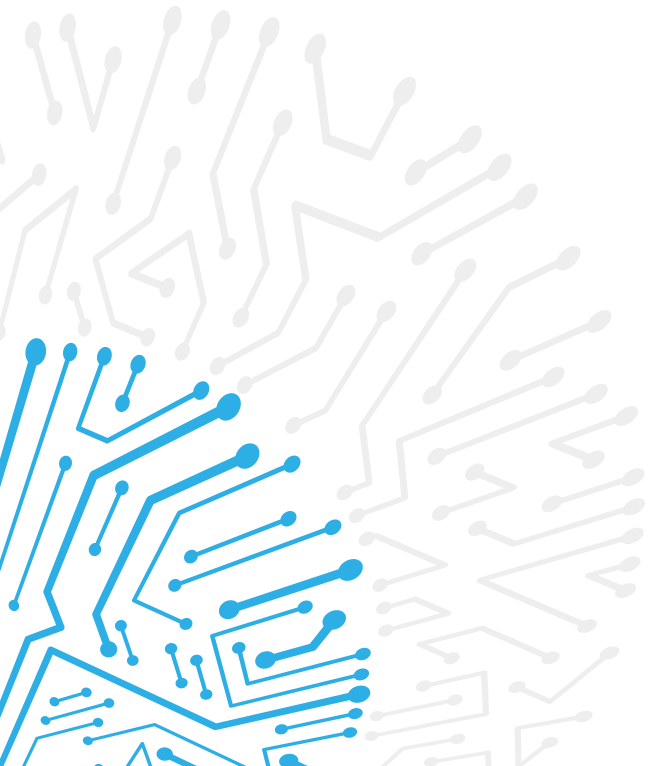
Koordinované zveřejňování zranitelností (Coordinated Vulnerability Disclosure) představuje formalizovaný proces dobrovolného objevování zranitelností v produktech informačních a komunikačních technologií (ICT produktech) třetími osobami (tzv. objeviteli), včetně notifikace objevené zranitelnosti vlastníkovi či správci ICT produktu za účelem provedení bezpečnostní opravy. **V současnosti v ČR neexistuje formalizovaný a ucelený pohled státu na koordinované zveřejňování zranitelností ani jeho specifická právní úprava.** NÚKIB tudíž během roku 2022 pracoval na návrhu národního přístupu, který umožní zodpovědné a koordinované objevování zranitelností využitelné pro orgány veřejné moci i soukromý sektor. Na podzim 2022 proběhlo několik jednání a konzultací se zástupci soukromého i veřejného sektoru za účelem identifikace relevantních právních i technických aspektů koordinovaného zveřejňování zranitelností a v prosinci 2022 byl poté připraven ke schválení návrh národní politiky koordinovaného zveřejňování zranitelností.

Nastavování bezpečnosti 5G sítí

NÚKIB spolu s Ministerstvem průmyslu a obchodu, Ministerstvem zahraničních věcí, Bezpečnostní informační službou, Úřadem pro zahraniční styky a informace a Vojenským zpravodajstvím v únoru 2022 vydal Doporučení pro hodnocení důvěryhodnosti dodavatelů technologií do 5G sítí v České republice. Doporučení poskytuje vodítko zejména pro dodávky do informačních a komunikačních systémů kritické infrastruktury ČR a představuje pohled státu, který se neodvíjí pouze od konečné technické podoby dodávaného řešení, nýbrž zohledňuje i netechnické aspekty – tedy podnikatelské, právní a politické prostředí, ve kterém se dodavatel pohybuje.

Bezpečnost dodavatelského řetězce

Na základě pověření Bezpečnostní rady státu NÚKIB v roce 2022 intenzivně pracoval na návrhu právní úpravy, která by měla významně omezit vliv rizikových dodavatelů v nejvýznamnější infrastruktuře ČR. Zákonná úprava má státu umožnit prověřovat dodavatele do své strategicky významné infrastruktury. Hlavním cílem této právní úpravy je zvýšit odolnost a bezpečnost ČR a omezit její závislost na potenciálně škodlivých zahraničních technologiích. **Hrozby v oblasti kybernetické bezpečnosti plynoucí z dodavatelských řetězců technologií jsou sice již dlouhodobě známy, dosud však v právním řádu ČR neexistuje komplexní právní úprava umožňující rizika plynoucí z těchto hrozeb cíleně vyhodnocovat a snižovat.**

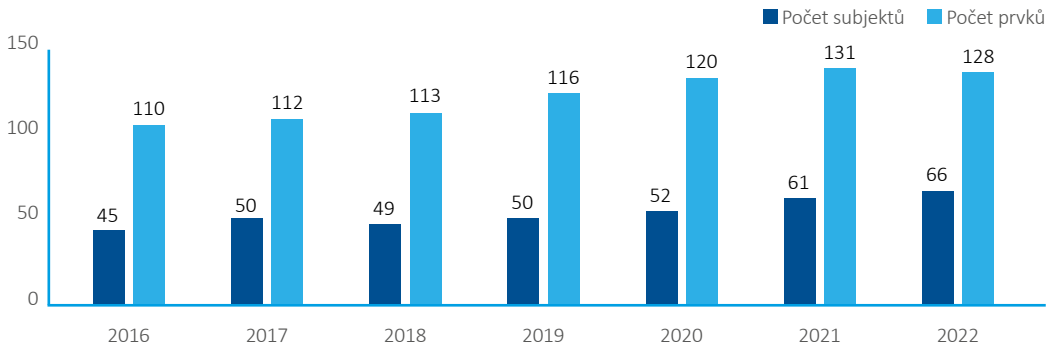


LEGISLATIVNÍ UKOTVENÍ: PŘÍPRAVA NÁVRHU NOVÉHO ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI

Určování a přezkum kritické informační infrastruktury, významných informačních systémů a informačních systémů základních služeb

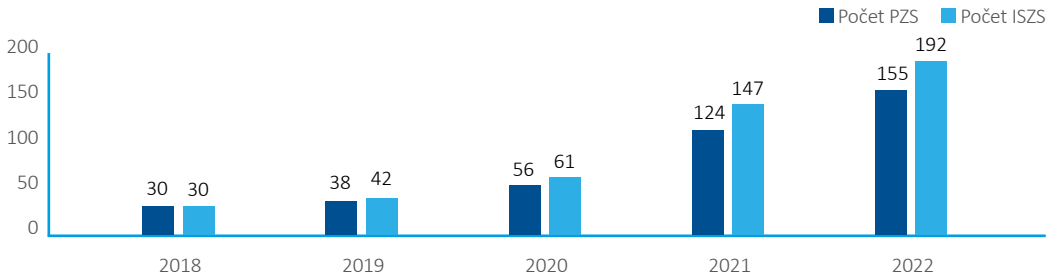
Určování KII provádí NÚKIB na základě zmocnění uvedeném v zákoně o kybernetické bezpečnosti a v krizovém zákoně, v souladu s nařízením vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, ve znění pozdějších předpisů, a to již od roku 2015. Zákon o kybernetické bezpečnosti také ukládá NÚKIB povinnost ověřovat každé dva roky aktuálnost určení prvků KII. Prvkem KII je pak informační nebo komunikační systém, který naplňuje kritéria daná výše uvedeným nařízením, ta určují jeho důležitost pro zachování vitálních funkcí státu. Správci prvků KII jsou jak organizační složky státu, tak i soukromé subjekty.

I v roce 2022 se tak NÚKIB věnoval určování nových a přezkumu stávajících prvků KII. **V roce 2022 bylo určeno 14 nových správců KII v soukromém i veřejném sektoru a došlo k přezkumu prvků u 19 správců KII, kteří byli určeni v předchozích letech.** NÚKIB tak k 31. prosinci 2022 evidoval celkem 66 subjektů, které spravují 128 prvků KII (viz Graf 30).



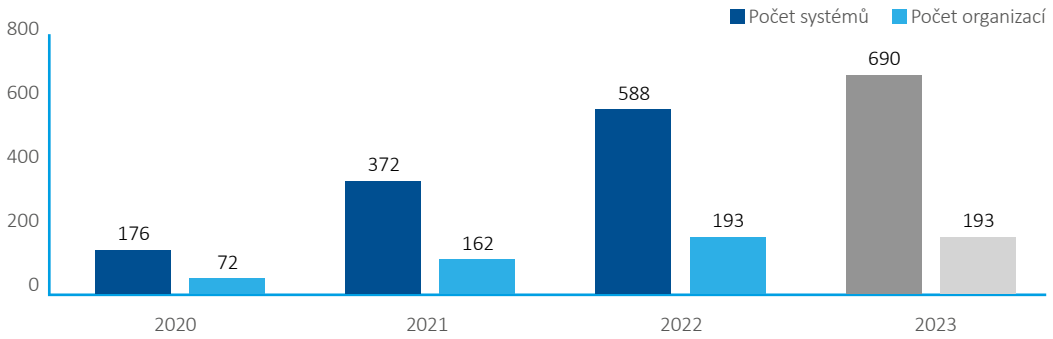
Graf 30: Vývoj počtu subjektů a prvků KII mezi lety 2016 až 2022

Minulý rok nadále pokračovalo i určování provozovatelů základní služby (PZS) a jejich informačních systémů základní služby (ISZS). V roce 2022 bylo určeno 31 nových provozovatelů základní služby, přičemž 9 správních řízení bylo ukončeno rozhodnutím o neurčení. NÚKIB tak v současné době eviduje celkem 155 provozovatelů základní služby, kteří dohromady spravují 192 informačních systémů základní služby (viz Graf 31).



Graf 31: Vývoj počtu PZS a ISZS mezi lety 2018 až 2022

V roce 2022 vešla v účinnost další část vyhlášky o významných informačních systémech a do regulace tak byly zahrnuty nové dva typy informačních systémů, které jsou přítomné v majoritě státních organizací, tedy informační systémy zajišťující výkon spisové služby a vedení elektronické úřední desky. Z tohoto důvodu došlo k nárůstu v počtu významných informačních systémů (VIS) z původních 372 (u 162 subjektů) na 588 významných informačních systémů u 193 subjektů. Pro rok 2023 odhaduje NÚKIB nárůst počtu významných informačních systémů na celkem 690 (viz Graf 32).



Graf 32: Vývoj počtu VIS mezi lety 2020 až 2022 + predikce vývoje pro rok 2023

Nový zákon o kybernetické bezpečnosti

Nejzásadnější činností NÚKIB v regulatorní oblasti byly práce na návrhu nového zákona o kybernetické bezpečnosti a prováděcích předpisů v souvislosti se směrnicí Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2).

V rámci přípravy na tuto zásadní legislativní změnu, jejíž účinnost se předpokládá od podzimu 2024, bylo zřízeno pět interních expertních skupin, ve kterých přes více než 40 zaměstnanců NÚKIB připravilo návrhy nového zákona o kybernetické bezpečnosti a jeho prováděcích předpisů. Vedle toho byla spuštěna první kola konzultací s odbornou veřejnosti a v této věci bylo osloveno 25 komor, sdružení a svazů reprezentujících či zastupujících subjekty, jichž se regulace kybernetické bezpečnosti dotýká nebo dotýkat bude. Každému oslovenému svazu či sdružení byla představena budoucí regulace a zároveň byl dán prostor na první kolo připomínek. Další jednání jakož i zveřejnění kompletních návrhů legislativních textů proběhnou v roce 2023.

V souvislosti s připravovanými legislativními změnami byl také spuštěn specializovaný web zaměřený na oblast směrnice NIS 2 a jejího promítnutí do národní regulace (viz Nová směrnice EU o bezpečnosti sítí a informací).

Evropské certifikace kybernetické bezpečnosti

V oblasti evropských certifikací kybernetické bezpečnosti na základě nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentura Evropské unie pro kybernetickou bezpečnost"), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („Akt o kybernetické bezpečnosti") došlo v roce 2022 k ustavení NÚKIB vnitrostátním orgánem certifikace kybernetické bezpečnosti, a to zákonem č. 226/2022 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů. Dále pak zákon upravuje některé aspekty správního řízení o tzv. autorizaci a stanoví skutkové podstaty přestupků spočívajících v porušení povinností stanovených Aktem o kybernetické bezpečnosti.

Na podzim byla zpracována strategie zajištění evropských certifikací kybernetické bezpečnosti se zaměřením nejenom na zajištění úkolů vyplývajících z čl. 58 Aktu o kybernetické bezpečnosti, ale také na podporu vzniku certifikačních orgánů a zkušebních laboratoří v souladu s Koncepcí rozvoje NÚKIB. Na přelomu roku 2022 a 2023 byl také připraven mikroweb pro evropské certifikace kybernetické bezpečnosti (EU Certifikace). Obsah stránek je koncipován tak, aby návštěvníkovi poskytl základní informace k evropským certifikacím kybernetické bezpečnosti, ale též zdroje pro detailnější informace.

Legislativní změny v oblasti cloud computingu a posuzování splnění bezpečnostních kritérií

Ministerstvo vnitra od srpna 2020 posuzuje poskytovatele cloud computingu a služby cloud computingu. NÚKIB v této oblasti provádí posouzení splnění bezpečnostních kritérií, která musí poskytovatelé cloud computingu splnit, aby mohli dodávat služby do veřejné správy.

Za rok 2022 provedl NÚKIB 43 posouzení dle přechodných ustanovení právního stavu účinného do 1. září 2021. Dle právního stavu účinného od 1. září 2021 provedl dále 46 posouzení poskytovatelů cloud computingu z hlediska jejich způsobilosti zajistit základní úroveň ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy a 27 posouzení způsobilosti poskytovatelů cloud computingu z hlediska veřejného pořádku, bezpečnosti a dodržování práv třetích osob.

DOZOROVÁ ČINNOST NÚKIB V ROCE 2022

Rok 2022 byl z pohledu auditní a kontrolní činnosti NÚKIB ovlivněn zejména eskalací geopolitické situace ve světě. NÚKIB se proto při auditní a kontrolní činnosti v roce 2022 zaměřil, mimo jiné, i na nejkritičtější systémy státní správy, u nichž byla provedena kontrola v oblasti řízení kontinuity činností.[7] Zmíněným organizacím bylo navíc nabídnuto a provedeno přizpůsobené table-top cvičení pokrývající právě tuto oblast.

Celkem bylo v roce 2022 provedeno 20 auditů a kontrol podle vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů. V rámci běžné kontroly nebo auditu je rámcově ověřováno cca 150 kontrolních bodů a na této činnosti se podílí čtyři až šest zaměstnanců NÚKIB v závislosti na velikosti subjektu, složitosti kontrolovaných systémů či jiných podmínkách, které vyžadují specifické znalostní či personální zdroje NÚKIB. Kontrola nebo audit od zahájení po ukončení trvá přibližně dva až tři měsíce.

Nejčastější nedostatky identifikované v průběhu kontrolní a auditní činnosti

- Nastavený systém zajišťování kybernetické bezpečnosti nepokrývá požadavky všech zainteresovaných stran;
- subjekty nedostatečně řídí aktiva a rizika spojená s kybernetickou bezpečností;
- bezpečnostní politiky a bezpečnostní dokumentace se často neaplikují v praxi nebo jsou neaktuální;
- subjekty nedostatečně řídí rizika spojená s dodavateli;
- používání zastaralého hardwaru a softwaru, který již jeho výrobce nepodporuje a neřízení souvisejících rizik;
- nedostatek odborníků na kybernetickou bezpečnost;
- nedostatečné vzdělávání zaměstnanců a osob zodpovědných za kybernetickou bezpečnost;
- nevhodná segmentace komunikační sítě.

[7] *Business contiunity – připravenost reagovat na krizové situace a schopnost minimalizovat případné následky takové situace.*

CVIČENÍ KYBERNETICKÉ BEZPEČNOSTI: CZ PRES A HEALTH CZECH

Národní cvičení	Počet účastníků	Mezinárodní cvičení
7	**504**	**3**

Rok 2022 byl ve znamení přípravy a následné realizace CZ PRES. NÚKIB uspořádal dvě netechnická cvičení kybernetické bezpečnosti, která měla za cíl připravit vybrané pracovníky Úřadu vlády ČR a dalších relevantních úřadů zapojených do příprav na CZ PRES na realistickou krizovou situaci v oblasti kybernetické bezpečnosti. Cvičení kladla důraz na ověření nastavených krizových komunikačních procesů a kanálů určených pro CZ PRES, a to také s ohledem na informování partnerů v EU.

Také v roce 2022 proběhla cvičení s mezinárodním přesahem. Prvním z nich bylo cvičení Locked Shields 2022. **Na tomto nejkomplexnějším cvičení kybernetické bezpečnosti na světě, které pořádá NATO Cooperative Cyber Defence Centre of Excellence v estonském Tallinu, se společný tým, složený z českých a slovenských specialistů na kybernetickou bezpečnost, umístil na 5. místě.** Za ČR se do společného týmu zařadili zástupci NÚKIB, CIRC Ministerstva obrany, EG.D, RedHat, CZ.NIC, České spořitelny a další odborníci z řad bezpečnostní komunity v ČR.

Dalším mezinárodním cvičením bylo Cyber Coalition. Jedná se o mezinárodní cvičení kybernetické bezpečnosti, které je pravidelně pořádáno NATO. Na úrovni ČR je koordinováno NÚKIB za civilní část a Velitelstvím kybernetických sil a informačních operací za vojenskou část. Samotný název cvičení podtrhuje jeho cíl – podporu silného společenství a vzájemné spolupráce. Toho je dosaženo pomocí scénářů, které sice obsahují technické výzvy, ale současně podněcují jednotlivé státy ke spolupráci a k vytvoření společného situačního povědomí. Na rozdíl od cvičení Locked Shields v tomto cvičení není žádný formální vítěz – cvičení je především o spolupráci, koordinaci a komunikaci v kontextu řešení krize vzešlé z kyberprostoru.

V závěru roku 2022 proběhlo druhé netechnické cvičení kybernetické bezpečnosti zaměřené na sektor zdravotnictví – Health Czech 2022. Cvičení bylo uspořádáno pro zdravotnická zařízení určená jako provozovatelé základních služeb. Zástupci z každého subjektu v rámci jednoho týmu odpovídali na otázky vycházející z připraveného scénáře a společně diskutovali o různých aspektech kybernetické bezpečnosti. Vedle týmů zastupujících zdravotnická zařízení se pak cvičení v rámci tzv. skupiny odborníků zúčastnili i zástupci NÚKIB a dalších přizvaných institucí (Úřad pro ochranu osobních údajů, Policie ČR, CZ.NIC) rovněž relevantních při zvládání a řešení krize.

Výhled budoucího směřování cvičení kybernetické bezpečnosti

NÚKIB se i nadále bude zaměřovat na rozvoj konceptu „train-the-trainer“, jehož cílem je prostřednictvím konzultací a pracovních setkání poskytovat podporu subjektům v tvorbě jejich vlastních cvičení kybernetické bezpečnosti. To bude nejen přínosné, ale také nutné zejména v budoucnu, kdy v návaznosti na směrnici NIS 2 dojde k výraznému nárůstu regulovaných subjektů a tím pádem také případných zájemců o provedení cvičení.

OSVĚTA A VZDĚLÁVÁNÍ V ČR: POZITIVNÍ VÝVOJ VE VZDĚLÁVACÍM SEKTORU

Vzdělávání, osvěta a prevence v oblasti kybernetické bezpečnosti byly v průběhu roku 2022 důležitými celospolečenskými tématy. I nadále přetrvávala potřeba připravenosti občanů ČR k bezpečnému používání digitálních technologií a pohybu v online světě napříč všemi sociálními skupinami jak při výkonu pracovních činností, tak při studiu nebo ve volném čase. **Nad běžný rámec vzdělávání zaměstnanců veřejné správy proběhla i příprava zaměstnanců organizací podílejících se v průběhu roku 2022 na zabezpečení CZ PRES.**

POČET ABSOLVENTŮ E-LEARNINGOVÝCH KURZŮ NÚKIB	
Dávej kyber!	40 592
Šéfuj kyber!	603
Kyber nemocnice!	9 641
Bezpečně v kyber!	850

Osvěta v rámci vzdělávacího sektoru

Vzdělávání v oblasti kybernetické bezpečnosti na úrovni základních a středních škol již několik let prochází pozitivním vývojem. V roce 2022 probíhala implementace revidovaného rámcového vzdělávacího programu pro základní vzdělávání a pro střední odborné vzdělávání. Změny byly zaměřeny na zavádění nové informatiky a digitálních kompetencí do výuky. **Dále pokračovaly práce na tzv. velké revizi rámcového vzdělávacího programu pro základní školy, kde se bude oblast kybernetické bezpečnosti rozvíjet v rámci digitálních kompetencí.**

U vybraných středních škol pokračují pokusná ověřování související s kybernetickou bezpečností. Jde například o pokusné ověřování vzdělávání podle školního vzdělávacího programu zaměřeného na kybernetickou bezpečnost zpracovaného podle rámcového vzdělávacího programu oboru vzdělání 18-20-M/01 Informační technologie a pokusné ověřování zaměřené na uznávání mezinárodních certifikačních standardů ICT v rámci profilové části maturitní zkoušky.

U vysokých škol pokračuje trend mírného růstu počtu studentů studijních programů informačních a komunikačních technologií. Naopak negativním trendem je nedostatečný nárůst počtu připravovaných nebo otevíraných studijních programů zaměřených na kybernetickou bezpečnost.

Ve spolupráci s Ministerstvem školství mládeže a tělovýchovy byl připraven i kurz základů kybernetické bezpečnosti pro pedagogy. Jeho úkolem je pomoci učitelům rozpoznávat rizikové jevy spojené s internetem a lépe zabezpečit on-line výuku.

Festival bezpečného internetu 2022

Při příležitosti Evropského měsíce kybernetické bezpečnosti NÚKIB zorganizoval Festival bezpečného internetu. Do festivalu se zapojilo 34 partnerů z neziskové i komerční sféry, kteří realizovali dohromady 37 aktivit pro různé cílové skupiny. Na realizaci 15 aktivit se podílel NÚKIB. Festival získal mediální podporu stanic Českého rozhlasu a osvětové spoty byly v průběhu října vysílány na stanicích ČRo Radiožurnál, ČRo Dvojka a ČRo Vltava. **Součástí festivalu bylo zveřejnění kurzu kybernetické bezpečnosti pro seniory (pomůcka SENIOR), který jim usnadňuje rozpoznávání škodlivých a nebezpečných e-mailů.** Od zveřejnění bylo evidováno 78 000 přístupů do kurzu. V rámci festivalu proběhla tzv. výtahová kampaň zaměřená na zdravotnický personál nemocnic. Zapojilo se 51 nemocnic a zdravotnických zařízení.

Osvěta v rámci zdravotnického sektoru

NÚKIB po předchozí analýze doplnil on-line vzdělávání pro sektor zdravotnictví o kurz Startuj kyber! Zároveň došlo k obsahové a designové aktualizaci kurzu Dávej kyber! pro zdravotnictví. Oba výše zmíněné kurzy absolvovalo 9 641 zaměstnanců z 27 nemocnic a zdravotnických zařízení. To je o celkem 5 051 proškolených osob více než v roce 2021.

Konference CyberCon 2022

V září 2022 NÚKIB uspořádal v brněnském Univerzitním kině Scala a na půdě Fakulty sociálních studií Masarykovy univerzity již osmý ročník konference CyberCon Brno. Hlavním cílem konference je poskytnout prostor pro propojení veřejného, akademického a soukromého sektoru v oblasti kybernetické bezpečnosti. Během třídenního programu si na 500 účastníků z řad odborné i široké veřejnosti mohlo poslechnout přednášky i diskuse reflektující technické, politické i právní aspekty kybernetické bezpečnosti. **Novinkou osmého ročníku byl workshopový den, během kterého si účastníci mohli prakticky vyzkoušet řešení problémů a výzev souvisejících s kybernetickou bezpečností.** Současně v rámci prvního dne celé akce proběhl i druhý ročník veletrhu studijních příležitostí Studuj kyber! určený pro studenty základních a středních škol.

Druhý den konference byl věnován aktuálním novinkám z oblasti regulace. Odborníci přiblížili chystanou směrnici NIS 2, analýzu rizik a sdíleli hlavní poznatky z auditů kybernetické bezpečnosti. V rámci závěrečného dne pak byly představeny strategické pohledy na různorodé výzvy v kybernetické bezpečnosti. Rovněž proběhla i politická diskuse, ve které oslovení poslanci Parlamentu ČR diskutovali nad financováním kybernetické bezpečnosti nebo nad rolí státu při jejím zajišťování.

Záznam z konference lze nalézt na webu www.cybercon.cz.

MEZINÁRODNÍ SPOLUPRÁCE: CZ PRES A SMĚRNICE NIS 2

Vývoj v oblasti kybernetické bezpečnosti v ČR je do značné míry svázaný s vývojem v zahraničí a rozhodnutími přijímanými nejen na úrovni EU, nýbrž i prostřednictvím dalších mezinárodních subjektů. Česká republika aktivně vystupovala v řadě mezinárodních organizací a integračních uskupení, zejména v EU, OSN, NATO, OECD, OBSE a ITU.

Evropská unie

Rok 2022 byl v oblasti mezinárodní spolupráce ovlivněn zejména CZ PRES, jehož se ČR podruhé v historii ujala 1. července 2022 na období šesti měsíců. První polovina roku 2022 proto byla věnována především intenzivním přípravám jak po obsahové, tak organizační stránce a zahrnovala množství jednání s partnery na národní i unijní úrovni.

Počínaje okamžikem převzetí předsednictví se ČR na půdě Rady EU věnovala řadě legislativních i nelegislativních dokumentů v oblasti kybernetické bezpečnosti. **Podařilo se dosáhnout obecného přístupu Rady EU k návrhu nařízení, kterým se stanoví opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti v orgánech, institucích a jiných subjektech Unie, tedy společné pozice všech členských států k tomuto návrhu.** Návrh nařízení si klade za cíl zvýšení úrovně kybernetické bezpečnosti unijních subjektů, a tím i posílení bezpečnosti napříč EU. **Započato bylo rovněž vyjednávání návrhu Aktu o kybernetické odolnosti[8], který stanovuje kyberbezpečnostní požadavky pro širokou škálu produktů s digitálními prvky s cílem zajistit jejich kybernetickou bezpečnost, a to v rámci celého jejich životního cyklu.** Vzhledem k tomu, že uvedené nařízení bude mít významný dopad na trh s produkty obsahujícími digitální prvky, bylo během podzimu konzultováno nejen s národními partnery v rámci státní správy, ale také se zástupci soukromého sektoru, na něž regulace dolehne nejvíce.

Mimo uvedené legislativní návrhy se ČR věnovala rovněž tématu posilování bezpečnosti dodavatelského řetězce informačních a komunikačních technologií (ICT). Hlavním úspěchem v této oblasti bylo přijetí závěrů Rady k bezpečnosti dodavatelského řetězce ICT, které iniciovali a na půdě Rady EU dojednali právě zástupci ČR. Přijetím těchto závěrů všech 27 členských států potvrdilo důležitost bezpečnosti dodavatelského řetězce ICT a potřebnost jeho posílení napříč EU prostřednictvím konkrétních navrhovaných kroků. Jde o významný milník v oblasti kybernetické bezpečnosti. Pozornost na půdě Rady EU však byla věnována i řadě dalších otázek, mimo jiné např. množství iniciativ v oblasti kybernetické diplomacie, kde NÚKIB úzce spolupracoval s Ministerstvem zahraničních věcí.

Pro kybernetickou bezpečnost a zejména budoucí podobu národní regulace mělo na úrovni EU zásadní význam přijetí směrnice NIS 2. Obsah směrnice byl vyjednán ještě v první polovině roku 2022, během francouzského předsednictví v Radě EU. **Finální znění textu směrnice NIS 2 po jazykových revizích pak bylo přijato během CZ PRES, a to koncem roku 2022. Součástí právních řádů členských zemí EU pak má být tato směrnice do 21 měsíců od chvíle, kdy vstoupila v platnost. Mělo by se tak tedy stát nejpozději v říjnu 2024.**

[8] *Cyber Resilience Act*

CZ PRES se však kromě vlastní činnosti Rady EU promítlo též do chodu řady expertních skupin v oblasti kybernetické bezpečnosti, jimž NÚKIB po tuto dobu předsedal a organizoval jejich jednání.

NÚKIB dále v průběhu CZ PRES pořádal řadu akcí v ČR i v zahraničí. **Nejvýznamnější událostí byla z tohoto pohledu dvoudenní předsednická konference EU Secure and Innovative Digital Future,** na jejíž organizaci NÚKIB pracoval společně s Ministerstvem průmyslu a obchodu a Úřadem vlády ČR, v koordinaci s Ministerstvem zahraničních věcí.

Konference EU Secure and Innovative Digital Future

První den konference s názvem Prague Cyber Security Conference 2022 byl v režii NÚKIB a navázal na tradici Prague 5G Security Conference konané v předchozích letech. Zúčastnilo se jí přes 500 expertů v oblasti kybernetické bezpečnosti z více než 80 zemí světa, kteří byli přítomni fyzicky v Praze nebo se připojili online. Mezi řečníky pak vystoupili čeští i zahraniční zástupci vlád a státního sektoru, mezinárodních organizací, jako je EU a NATO, ale i různých think-tanků. **Hlavním tématem byla bezpečnost dodavatelského řetězce ICT, její vývoj, výzvy, které přináší, i možné způsoby realizace**.

Druhý den konference nazvaný Towards a Secure and Innovative Ecosystem pak probíhal pod záštitou Ministerstva průmyslu a obchodu ČR a Úřadu vlády ČR a věnoval se zejména bezpečnosti nových technologií, například umělé inteligenci či otázce bezpečných toků dat v rámci EU i mimo ni.

Kromě konference a řady pracovních jednání expertních skupin, uspořádal NÚKIB také několik vzdělávacích a společenských akcí, to vše za účasti zahraničních partnerů nejen z členských států či unijních institucí.

Další mezinárodní organizace

Česká republika se v uplynulém roce aktivně účastnila jednání Otevřené pracovní skupiny OSN k bezpečnosti informačních a komunikačních technologií (OEWG), ve kterém společně s dalšími liberálními demokraciemi bránila snahám autoritářských režimů posílit státní kontrolu nad správou internetu a online obsahem a omezit lidská práva v kybernetickém prostoru. Česká republika dlouhodobě podporuje otevřený, svobodný, bezpečný, stabilní a přístupný kybernetický prostor. Spolu se společností Microsoft a CyberPeace Institute se ČR podílela též na mezinárodním projektu Protecting the Healthcare Sector from Cyber Harm zaměřeného na ochranu zdravotnického sektoru. Závěrem byla sada doporučení vydaných ve formě Kompendia představeného na okraj třetího jednání OEWG v New Yorku.

Česká republika se ve spolupráci s dalšími stejně smýšlejícími zeměmi podílela na rozvoji kybernetických kapacit ve třetích zemích. Konkrétně uskutečnila projekty v Bosně a Hercegovině, Moldavsku, Indonésii, Senegalu a Ghaně.

NÚKIB se taktéž aktivně podílel i na činnosti neformální skupiny na bezpečnost ICT při OBSE. Tento rok se mimo jiné zapojil do přezkumu nového e-learningového kurzu na téma politiky koordinovaného zveřejňování zranitelností nebo vystoupil v rámci side-eventu k národním praktikám při řešení kybernetických incidentů.

VÝHLED TRENDŮ V KYBERNETICKÉ BEZPEČNOSTI V ČR NA ROKY 2023 A 2024

Hrozby v energetice a dopravě

Jedním z trendů uplynulého roku se stal zvýšený zájem škodlivých útočníků o sektory energetiky a dopravy. Jejich význam zásadně narostl spolu s počátkem ruské invaze na Ukrajinu a souvisejícími událostmi, čehož brzy začali zneužívat jak státní či státem podporovaní aktéři, tak i kyberkriminální či hacktivistická uskupení. **Je pravděpodobné (55–70 %), že v následujícím období dojde k méně či více závažným útokům na subjekty spadající do energetického a dopravního sektoru.** Riziko takových útoků bude velmi pravděpodobně (75–85 %) narůstat v návaznosti na politická rozhodnutí a jiný vývoj spojený s rusko-ukrajinskou válkou.

Perzistence kampaní

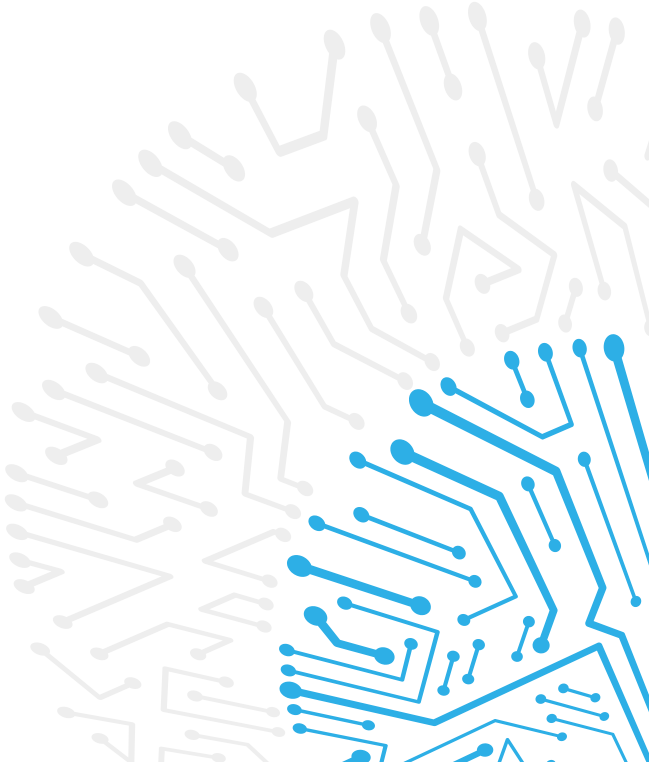
Česká republika se v roce 2022 potýkala s více perzistentními kampaněmi. V prvním případě se jednalo o vishing, pomocí něhož byli napadení uživatelé naváděni k instalaci vzdálené správy na své počítače. Druhou perzistentní kampaní byl phishing distribuovaný pomocí SMS zpráv cílený na bankovní identitu a následnou krádež finančních prostředků. Obě kampaně se vyznačovaly vytrvalostí útočníků, kteří i přes aktivní zásahy různých složek pokračovali v útocích. **Lze tak sledovat trend, kdy útočníci po vzoru moderního vývoje nasazují automatizovanější metody tvorby infrastruktury, aby udrželi kampaň v chodu i v případě proaktivních zásahů. Sledujeme a očekáváme také pokračování trendu sofistikovanosti útočníků, zejména v oblasti věrohodnosti podvodných e-mailů či webových stránek využitých při útocích.**

Ransomware

NÚKIB eviduje ransomwarové incidenty téměř každý měsíc, přičemž daný trend bude pokračovat téměř jistě (90–100 %) i v dalších letech. Nyní již převládá ransomware nabízený ve formě služby (ransomware-as-a-service), jenž obvykle operuje na bázi vícenásobného vydírání (exfiltrace dat, možnost jejich zveřejnění/prodeje či další aktivity cílené na zvýšení tlaku platit výkupné). **Přestože ransomware je primárně doménou kyberkriminálních skupin, tak s ohledem na vybrané státy pod sankčními mechanismy nelze vyloučit (25–50 %), že i ony jej začnou využívat, ať už pro finanční zisk, či zastírání reálných destruktivních nebo kyberšpionážních cílů.** Dále existuje i reálná možnost (25–50 %) spolupráce nestátních a státních aktérů, kdy nestátní aktéři získají finanční prostředky a státní aktéři přístup k exfiltrovaným informacím spolu vyšší mírou věrohodného popření (tzv. plausible deniability).

Kybernetické útoky proti strategickým institucím státu

Veřejná správa zahrnující mj. i strategické instituce státu je dlouhodobě nejčastěji zasaženým sektorem, přičemž je téměř jisté (90–100 %), že tomu tak bude i v následujícím období. Vyjma možnosti zisku zpravodajsky cenných informací mohou být motivace útočníků ovlivněny také geopolitickou situací. **V kontextu ČR je významným faktorem primárně ruská invaze na Ukrajinu a dále česká podpora napadené země spolu s aktivním členstvím v EU/NATO.** Též nelze vyloučit (25–50 %), že vybrané instituce mohou být dlouhodobě kompromitovány, přičemž průnik nebyl identifikován vzhledem k pokročilosti útočníků.



PLNĚNÍ CÍLŮ NÁRODNÍHO PLÁNU VÝZKUMU A VÝVOJE V KYBERNETICKÉ A INFORMAČNÍ BEZPEČNOSTI ZA ROK 2022

V rámci plnění cílů tohoto plánu NÚKIB uspořádal tři setkání Platformy pro výzkum a vývoj v kybernetické bezpečnosti, jejímiž členy jsou orgány státní správy, akademické a výzkumné instituce a zástupci soukromého sektoru. První setkání proběhlo v prostorách Technologické agentury ČR, druhé na půdě Vysoké školy báňské – Technické univerzity Ostrava. Obě tato setkání byla zaměřena na posílení spolupráce v oblasti výzkumu a vývoje. Třetí setkání bylo realizováno na Fakultě informatiky Masarykovy univerzity a zaměřilo se na aktuální trendy v oblasti kryptografie a na vývoj kvantových technologií.

NÚKIB dále podporoval vyšší zapojení uživatelské komunity do systému podpory výzkumu, vývoje a inovací v kybernetické bezpečnosti, včetně posílení schopnosti zavádět výsledky do praxe. NÚKIB spolu s dalšími útvary Policie ČR a Armády ČR podpořil z pozice aplikačního garanta několik výzkumných projektů financovaných z programů veřejných soutěží Ministerstva vnitra. V rámci mezinárodních projektových iniciativ se NÚKIB stal členem konsorcia projektu vedeném Masarykovou univerzitou s názvem Cyber-security Excellence Hub in Estonia and South Moravia (CHESS), jehož cílem je rozvinout výzkumnou a inovační spolupráci Jihomoravského kraje s Estonskem v oblasti kyberbezpečnosti.

I v roce 2022 NÚKIB pokračoval v budování informačního zázemí v oblasti výzkumu a vývoje v kybernetické bezpečnosti. Na webových stránkách NÚKIB jsou pravidelně publikovány newslettery zaměřené na novinky v oblasti podpory vědy a výzkumu či nové technologie v kybernetické bezpečnosti. Pomocí nástroje vědecké diplomacie NÚKIB uspořádal videokonferenční setkání zástupců akademické sféry se svými izraelskými protějšky s cílem navázat užší spolupráci vedoucí k případné přípravě mezinárodního výzkumného projektu. NÚKIB rovněž poskytl několik neformálních konzultací týkajících se možnosti čerpání finančních prostředků z rámcových programů EU.

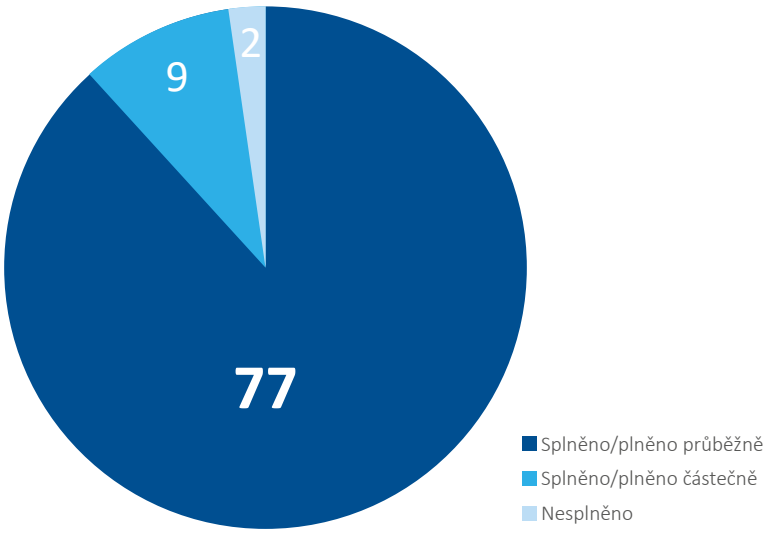
Prostřednictvím pracovních skupin Evropské komise se NÚKIB podílel na struktuře a tematickém zaměření rámcového programu Digitální Evropa, jehož prostřednictvím Evropská komise rozděluje finanční prostředky do oblastí rozvoje umělé inteligence, superpočítačů, kybernetické bezpečnosti či pokročilých digitálních dovedností.

PŘÍLOHA 1: VYHODNOCENÍ AKČNÍHO PLÁNU K NÁRODNÍ STRATEGII KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY ZA ROK 2022

Rok 2022 byl druhým rokem vyhodnocování Akčního plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025 (dále jen „Akční plán"). NÚKIB nejenže koordinuje vyhodnocení celého Akčního plánu, ale podílí se z pozice gestora/spolupracujícího subjektu na plnění 101 z celkových 105 úkolů. Pro rok 2022 bylo předmětem vyhodnocení 88 úkolů. Z těchto úkolů je 73 v režimu průběžného plnění.

Z hodnocených úkolů bylo 77 splněno nebo plněno průběžně. Devět úkolů bylo splněno částečně, jako nesplněné byly vyhodnoceny dva úkoly. Oproti roku 2021 (8 částečně splněných, 0 nesplněných úkolů) se tak jedná o mírný pokles v úspěšnosti plnění Akčního plánu. Příkladem úkolu termínovaného a splněného v roce 2022 bylo *vypracovat metodický dokument k řízení bezpečnosti dodavatelů a poskytnout ho orgánům a osobám povinným podle zákona o kybernetické bezpečnosti.* NÚKIB za konzultací s Ministerstvem financí, Ministerstvem vnitra a Ministerstvem průmyslu a obchodu zpracoval metodický dokument, v němž byly zohledněny i podpůrné materiály Ministerstva pro místní rozvoj týkající se veřejných zakázek. Vznikl tak materiál zabývající se řízením dodavatelů v průběhu celého životního cyklu dodávky, zohledňující i specifika dodavatelských vztahů podle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů. V prosinci 2022 byl materiál rozeslán povinným osobám, přičemž během roku 2023 má být zveřejněn na webu NÚKIB. Naopak příkladem nesplněného úkolu *byla tvorba a organizace cvičení v oblasti kybernetické bezpečnosti pro zahraniční partnery ČR v koordinaci a synergii s dalšími mezinárodními aktivitami ČR.* Ačkoliv se NÚKIB v uplynulém roce na mezinárodních cvičeních v oblasti kybernetické bezpečnosti podílel, žádné konkrétní cvičení pro zahraniční partnery neproběhlo.

Za hlavní důvody negativně ovlivňující míru plnění Akčního plánu lze označit ruskou invazi na Ukrajinu a na to navázanou zhoršenou bezpečnostní situaci, která vyčerpávala personální a další kapacity pro plnění bezprostřednějších a nutnějších úkolů. Druhým faktorem pak byla příprava a realizace historicky druhého CZ PRES, které především ve druhé polovině roku vázalo značnou část personálních kapacit zejména v oblasti mezinárodní spolupráce. Příkladem úkolu, jehož plnění bylo kvůli CZ PRES upozaděno, bylo *vytvořit přehled implementace nezávazných norem odpovědného chování států v kyberprostoru a aktivně se podílet na prosazování jejich dodržování, bránit jejich rozmělňování a oslabování mj. v oblasti dodržování lidských práv.* Ač na národní úrovni za koordinace Ministerstva zahraničních věcí probíhala spolupráce s relevantními institucemi, do konce roku nedošlo k vytvoření uceleného přehledu nezávazných norem. Na částečně s/plněných a nesplněných úkolech se bude pracovat v roce 2023 tak, aby došlo k jejich plnohodnotnému naplnění.



Graf 33: Vyhodnocení úkolů Akčního plánu za rok 2022

ZDROJE:

- Microsoft. 2022. Microsoft Digital Defense Report 2022. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us

- Policie České republiky. 2022. Vývoj registrované kriminality v roce 2022. https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx

- Česká bankovní asociace. 2022. Kybernetických útoků dramaticky přibývá a jsou stále rafinovanější. ČBA proto spouští celonárodní vzdělávací kampaň #nePINdej!. https://cbaonline.cz/kybertest-2022

- NÚKIB. 2022. Hrozby a zranitelnosti. https://www.nukib.cz/cs/infoservis/hrozby/#1

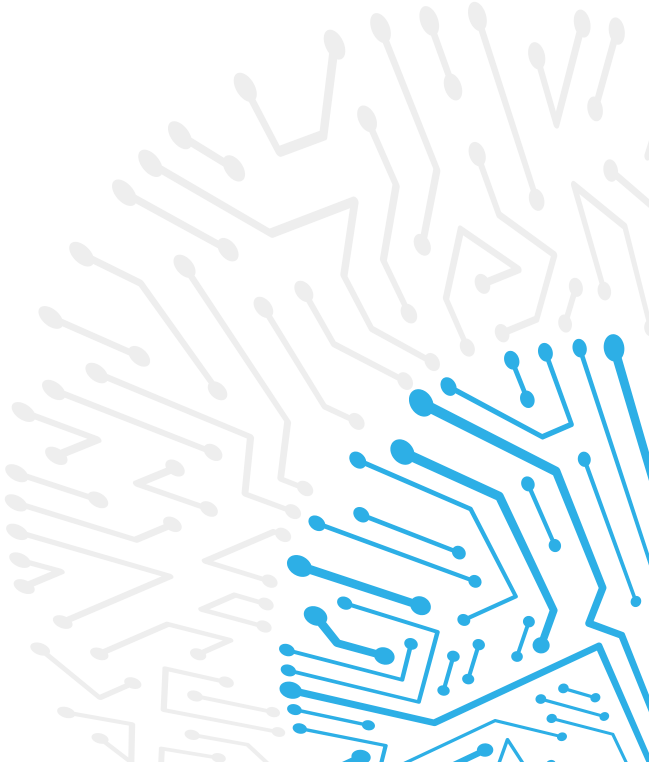
O NÚKIB

NÚKIB je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Dále má na starosti problematiku veřejně regulované služby v rámci družicového systému Galileo. NÚKIB vznikl 1. srpna 2017 na základě zákona č. 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

NÚKIB v současnosti pomáhá zajišťovat kybernetickou bezpečnost ČR a jejích obyvatel prostřednictvím:

- poskytování včasných, jasných a relevantních informací subjektům kritické informační infrastruktury, provozovatelům základní služby i orgánům veřejné správy;
- zajišťování bezpečnosti utajovaných informací v informačních a komunikačních systémech včetně kryptografické ochrany;
- přípravy národních bezpečnostních standardů, zákonů a podzákonných norem v oblasti kybernetické bezpečnosti;
- poskytování technické pomoci a dalších služeb, např. prověření zabezpečení pomocí technik penetračního testování nebo poskytování skenů zranitelností;
- vedení operativní reakce na kybernetické incidenty s využitím expertizy a přístupu k informacím pro efektivní zvládnutí incidentů;
- pořádání tréninků a kybernetických cvičení na národní i mezinárodní úrovni;
- analýzy trendů v oblasti kybernetické bezpečnosti;
- poskytování metodické podpory, vzdělávání a osvěty v tématech spojených s oblastí kybernetické bezpečnosti;
- provádění výzkumu a vývoje v oblasti kybernetické bezpečnosti;
- vyhodnocování rizik v oblasti kybernetické bezpečnosti a přijímání příslušných nápravných a preventivních opatření;
- provádění kontroly dodržování požadavků zákona o kybernetické bezpečnosti u regulovaných osob;
- zastupování České republiky v orgánech mezinárodních organizací působících v oblasti kybernetické bezpečnosti;
- spolupráce s veřejným, soukromým a akademickým sektorem na národní i mezinárodní úrovni.

Pro více informací o NÚKIB navštivte naše webové stránky www.nukib.cz nebo sledujte aktuality z oblasti kybernetické bezpečnosti v ČR na našich sociálních sítích Twitter, LinkedIn, Facebook nebo Instagram. Záznamy z některých akcí, které NÚKIB pořádá, nebo se jich účastní jeho zástupci, pak najdete na YouTube kanálu NÚKIB.



NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost